
Movement Tracking System Trusted Facilities Manual

Version 2.0

10 October 2001

Distribution authorized to the Department of Defense (DoD) and U.S. DoD Contractors only to protect the technical data and operational data from automatic dissemination under the International Exchange Program or by other means, 16 March 2001. Refer other requests for this document to PM GCSS-Army, MTS Project Office, Fort Lee, Virginia

23801-1718

TABLE OF CONTENTS

TABLE OF CONTENTS	II
LIST OF TABLES:.....	VII
EXECUTIVE SUMMARY	1
1. INTRODUCTION.....	2
1.1. PURPOSE	2
1.2. SCOPE	2
1.3. DOCUMENT ORGANIZATION	3
2. SYSTEM SECURITY OVERVIEW.....	5
2.1. ARCHITECTURE DESCRIPTION	5
2.1.1. <i>Hardware Configurations</i>	5
2.1.2. <i>MTS Software Configurations</i>	7
2.1.3. <i>External Interfaces</i>	8
2.2. ACCREDITATION BOUNDARIES	8
2.3. SECURITY CONFIGURATION	8
2.4. PACKET SWITCH CONTROLLED ENVIRONMENT BOUNDARIES.....	8
2.5. PACKET SWITCH SECURITY CONFIGURATION ADMINISTRATION	8
2.6. ESTABLISHING THE MTS PACKET SWITCH SECURITY CONFIGURATION	9
2.6.1. <i>Snoop</i>	9
3. SECURITY ENVIRONMENT.....	10
3.1. PHILOSOPHY OF PROTECTION.....	10
3.2. THREATS TO SYSTEM SECURITY	11
3.2.1. <i>Human</i>	11
3.2.2. <i>Structural/environmental</i>	12
3.2.3. <i>Natural Disasters</i>	12
3.2.4. <i>Technical</i>	12
3.3. PHYSICAL SECURITY ASSUMPTIONS	12
3.3.1. <i>Surge Protection</i>	13
3.3.2. <i>Primary System Components Security</i>	13
3.3.3. <i>Secure Working Location</i>	14
3.3.4. <i>Secure Terminal Locations</i>	14
3.3.5. <i>Uninterruptible Power Supply (UPS)</i>	14
3.3.6. <i>Physical Security Standard Operating Procedures (SSOP)</i>	14
3.4. PERSONNEL SECURITY ASSUMPTIONS.....	14
3.5. PERSONNEL SECURITY TRAINING AND AWARENESS	14
3.6. SYSTEM SECURITY COUNTERMEASURES.....	15
3.7. POLICY BASED COUNTERMEASURES.....	16
3.8. COPYRIGHT LAWS.....	17
3.9. HARD AND SOFT COPY MARKINGS	17

4.	SECURITY ARCHITECTURE	18
4.1.	WINDOWS NT SECURITY ARCHITECTURE	18
4.2.	SECURITY REFERENCE MONITOR	18
4.3.	LOCAL SECURITY AUTHORITY	18
4.4.	SECURITY ACCOUNTS MANAGER.....	18
4.5.	DoD SECURITY BANNER	19
4.6.	LOGON PROCESS	19
4.7.	SCREEN SAVER ACCESS	19
4.8.	DISCRETIONARY ACCESS CONTROLS	20
4.9.	ACCESS TOKENS AND SECURITY IDENTIFIERS (SID).....	20
5.	PROTECTIVE MECHANISM FOR SYSTEM ADMINISTRATORS	21
5.1.	LOGGING ONTO MTS	21
5.1.1.	<i>Password Policy.....</i>	<i>21</i>
5.1.2.	<i>Password Guidelines</i>	<i>21</i>
5.1.3.	<i>Password Lifetime.....</i>	<i>22</i>
5.1.4.	<i>Root/Administration/Super-User Password Management.....</i>	<i>22</i>
5.1.5.	<i>Passwords and Shadow Files.....</i>	<i>22</i>
5.2.	SYSTEM BACKUP, RECOVERY, AND CONTINGENCY.....	23
5.2.1.	<i>System Backup</i>	<i>23</i>
5.3.	CONTINGENCY PLANNING.....	23
5.4.	SECURITY CONFIGURATION	23
5.5.	CONTROLLED OPERATING ENVIRONMENT	23
5.6.	SOFTWARE VERSION BASELINE CONTROL	23
5.7.	SITE MISSION-SPECIFIC SOFTWARE CONTROL	24
5.8.	CONTROLLED ENVIRONMENT BOUNDARIES.....	24
5.9.	SECURITY CONFIGURATION ADMINISTRATION	24
5.9.1.	<i>IAVA Protect Tools – C2 Tools.....</i>	<i>24</i>
5.9.2.	<i>Password Complexity Tool – C2 Tools.....</i>	<i>25</i>
5.10.	MCAfee ANTI-VIRUS SOFTWARE.....	25
6.	SYSTEM INSTALLATION FOR WINDOWS NT 4.0.....	26
6.1.	ACCOUNTABILITY	26
6.1.1.	<i>Windows NT 4.0.....</i>	<i>26</i>
6.1.2.	<i>Post-Service Pack 6 Hot-fixes for Windows NT 4.0</i>	<i>27</i>
6.1.3.	<i>User Accounts</i>	<i>27</i>
6.1.4.	<i>Account Policy</i>	<i>28</i>
6.1.5.	<i>Creating a New User Account</i>	<i>29</i>
6.1.6.	<i>Built-In Accounts</i>	<i>31</i>
6.1.7.	<i>Groups.....</i>	<i>32</i>
6.1.8.	<i>Built-In Groups</i>	<i>32</i>
6.1.9.	<i>Assigning User Profiles, Logon Scripts and Home Directories</i>	<i>34</i>
6.1.10.	<i>Administrator Accounts</i>	<i>37</i>
6.2.	SYSTEM POLICY	38
6.3.	USER RIGHTS POLICY	39
6.3.1.	<i>Recommended Rights Assignments</i>	<i>42</i>

6.4.	AUDIT AND ARCHIVE LOG POLICIES	42
6.4.1.	Enabling Auditing	43
6.4.2.	Auditing Directories and Files.....	44
6.4.3.	Auditing Printers.....	46
6.4.4.	Auditing the Registry.....	48
6.4.5.	Auditing Base Objects.....	50
6.4.6.	Auditing of Privileges	51
6.4.7.	Viewing Event Logs.....	53
6.4.8.	Setting Options for Log Events	54
6.4.9.	Alternative Locations for the Security Log	55
6.4.10.	Archiving the Logs	55
6.4.11.	Archiving Event Logs.....	56
6.4.12.	Verifying Saved Event Logs	57
6.4.13.	Clearing Event Logs	57
6.4.14.	Restoring Event Logs	58
6.4.15.	Recommendations for Auditing.....	59
6.5.	MANAGING PRINTERS	59
6.6.	SETTING REGISTRY SIZE LIMIT	60
6.7.	PERFORMANCE MONITOR	61
7.	ACCESS CONTROLS	65
7.1.	FILE SYSTEM ACCESS CONTROLS	65
7.1.1.	File Permissions.....	65
7.1.2.	Directory Access Permissions.....	66
7.1.3.	File and Directory Ownership.....	69
7.2.	REGISTRY ACCESS CONTROLS	70
7.3.	RECOMMENDED PERMISSIONS FOR FILES, DIRECTORIES, AND REGISTRY KEYS	72
7.4.	LOCKING THE WORKSTATION	72
7.4.1.	Automatic Locking	72
7.4.2.	Manual Locking	73
7.4.3.	Logging off the System.....	74
8.	SYSTEM INSTALLATION FOR MTS SOFTWARE	75
9.	UNIX SECURITY ARCHITECTURE FOR THE MTS NETWORK ADMINISTRATOR.....	76
9.1.	UNIX SECURITY ARCHITECTURE	76
9.2.	SYSTEM BACKUP	77
9.3.	SYSTEM RESTORE	78
10.	SYSTEM CONFIGURATION FILES.....	79
10.1.	/ETC./NSWITCH.CONF	79
10.2.	IP FORWARDING CONTROL (/ETC/RC2.D/S99INET)	79
10.3.	ANTI-VIRUS SOFTWARE.....	80
10.3.1.	McAfee Virus-Scan for Unix	80
10.3.2.	McAfee Virus-Scan for Windows NT	81
10.4.	VIRUS DEFINITION UPDATES	86
10.4.1.	Control Station Installation	86

10.4.2.	<i>V2 Installation</i>	87
11.	ACCESS CONTROL	88
11.1.	DISCRETIONARY ACCESS CONTROLS (DAC)	88
11.2.	LEAST PRIVILEGE CONCEPT	88
11.3.	ASSIGNING PERMISSIONS	88
11.4.	SET UID AND SET GID PROGRAMS	88
12.	SECURITY-RELEVANT FILES AND DIRECTORIES	90
12.1.	/ (ROOT) DIRECTORY	90
12.2.	/ETC DIRECTORY	90
12.3.	BINARY FILES	90
12.4.	AUDIT LOGS AND ONLINE ARCHIVES	91
12.5.	OTHER RELEVANT FILES.....	91
12.6.	UNAUTHORIZED FILE SYSTEM OBJECTS	91
12.7.	DEVELOPMENT TOOLS AND UTILITIES	92
12.8.	NON-MTS PACKET SWITCH SPECIFIC SOFTWARE	92
12.9.	.RHOSTS FILES.....	92
13.	MOUNTED FILE SYSTEM CONTROL	94
13.1.	USER PRIVILEGES	94
14.	LOCAL ACCOUNTS	96
15.	SITE-SPECIFIC RESPONSIBILITIES AND PROCEDURES	97
15.1.	SITE CHIEF/COMMANDERS.....	97
15.2.	DIRECT APPROVING AUTHORITY (DAA)	97
15.3.	INFORMATION ASSURANCE SECURITY OFFICER (IASO)	97
15.4.	SYSTEM ADMINISTRATOR (SA)	98
15.5.	NETWORK ADMINISTRATOR (NA)	99
15.6.	USERS	100
16.	COUNTERMEASURE PROCEDURES	102
16.1.	CONTROLLING MISUSE	102
16.2.	SOFTWARE CONTROLS	102
16.3.	MISUSE DETECTION	102
17.	ROOT ACCOUNT USAGE	104
18.	AUDIT MANAGEMENT	105
18.1.	GENERAL AUDIT CONCEPTS	ERROR! BOOKMARK NOT DEFINED.
18.2.	AUDIT DEFINITIONS	105
18.3.	AUDIT ONLINE ARCHIVE	106
18.4.	AUDIT LONG TERM ARCHIVE	106
18.5.	ARCHIVE LABELS.....	106
18.6.	AUDIT DEPOSITORY SPACE FULL CONDITIONS AND POLICY	106
18.7.	AUDIT EVENT REQUIREMENTS.....	107
18.8.	AUDIT LOG ANALYSIS	108
19.	CHANGE DES KEYS	110

LIST OF FIGURES

Figure 1	User Manger.....	28
Figure 2	Account Policy.....	28
Figure 3	New User Dialog Box.....	29
Figure 4	Group Memberships.....	30
Figure 5	User Profile	30
Figure 6	Domain Information.....	31
Figure 7	Local Groups.....	32
Figure 8	Profiles	36
Figure 9	Copy To	36
Figure 10	User Environment Profile	37
Figure 11	Renaming Users	37
Figure 12	System Policy Editor.....	38
Figure 13	User Rights Policy Dialog Box.....	42
Figure 14	Audit Policy	43
Figure 15	Auditing Directories & Files.....	44
Figure 16	Auditing Users/Groups for Directories & Files	45
Figure 17	Adding Users/Groups for Auditing Directory & Files	45
Figure 18	Auditing Users/Groups for Directories & Files	46
Figure 19	Auditing Dialog Box.....	47
Figure 20	Auditing Users/Groups for Printers	47
Figure 21	Adding Users/Groups for Auditing Printers	48
Figure 22	Auditing the Registry.....	48
Figure 23	Auditing Users/Groups for the Registry	49
Figure 24	Adding Users/Groups for Auditing the Registry	49
Figure 25	Audit Policy for Base Objects.....	50
Figure 26	Setting Registry Key Values	51
Figure 27	Setting Registry Key Values.....	52

Figure 28	Binary Editor Box	52
Figure 29	Viewing Event Logs	54
Figure 30	Options for Event Logs	54
Figure 31	Archiving Event Logs	56
Figure 32	Save As Option for Event Logs	56
Figure 33	Clearing Event Logs - #1	57
Figure 34	Clearing Event Logs - #2	58
Figure 35	Restoring Event Logs.....	58
Figure 36	Locating Archived Event Logs	59
Figure 37	System Properties.....	60
Figure 38	Registry Size Settings	61
Figure 39	Performance Monitor	62
Figure 40	Selecting Counters to Chart	63
Figure 41	Alert Monitoring	63
Figure 42	File Permission Dialog Box	66
Figure 43	Directory Permissions for Users/Groups	68
Figure 44	Taking Ownership of Files.....	69
Figure 45	Registry Editor	71
Figure 46	Registry Permissions.....	72
Figure 47	Screensaver Settings	73
Figure 48	Virus-Scan Console	81
Figure 49	Virus-Scan Detection Settings	82
Figure 50	Virus-Scan Action Settings.....	83
Figure 51	Virus-Scan Alert Settings	83
Figure 52	Virus-Scan Report Settings.....	84
Figure 53	Virus-Scan Exclusion Settings.....	85
Figure 54	Installing Anti-Virus Updates	86

LIST OF TABLES:

Table 1	MTS Hardware Configurations.....	5
---------	----------------------------------	---

Table 2	MTS Software System Configurations	7
Table 3	Built-In Groups	32
Table 4	System Groups	34
Table 5	User Profile Settings	35
Table 6	User Rights.....	39
Table 7	Binary Files.....	90
Table 8	Other Files.....	91
Table 9	Audit Requirements	107

EXECUTIVE SUMMARY

This trusted facilities manual (TFM) has been created for the Army movement tracking system (MTS). It identifies procedures for the secure configuration of the MTS running over Microsoft Window NT 4.0 (Service Pack 6 (SP6)) and service specific software provided by COMTEC.

The TFM has been created for system administrators (SA) charged with maintaining the Movement Tracking System in a secure manner. The term “system administrator” refers to any individual who has been granted administrative privileges and authority within the MTS. This guide covers the roles and responsibilities of the SA as they pertain to the MTS.

Four source documents that will be noted throughout the TFM. They are: Army Regulation 380-19, DII COE Security Software Requirements Specifications (SRS), Guide to Implementing Windows NT in Secure Networks Environments, Version 1.1, and Security Tips for Windows NT 4.0 Workstation with Service Pack 6.

1. INTRODUCTION

1.1. Purpose

The TFM is directed towards system and network administrators responsible for the MTS. Its goal is to provide guidelines for the secure configuration and maintenance of the MTS within the Department of Defense (DoD) standards. The TFM focuses on MTS Block I (sensitive but unclassified (SBU) information), but since the security requirements for Block I differ from those in Block II (classified SECRET information) it will also serve as the basis for a transition vehicle to Block II.

1.2. Scope

This document provides guidance to system administrative and security personnel for the implementation, configuration, and maintenance of the security features incorporated within the MTS. It also provides guidance for security management in compliance with system security policy and procedures. Other guidance:

- Configuration and installation of secure systems including servers and clients.
- Operation of a system in a secure manner.
- Operation of administrative personnel making effective use of the system's privileges and protection mechanisms.
- Dissemination of warnings concerning possible misuse of administrative authority

Because of the unique deployment of the MTS, this guide will focus on system administration in two areas. The first is that of the deployed SA, who is responsible for the security integration and operation of the mobile and portable (M&P) MTS units (Control station and V1 (System Delayed), and V2). These M&P-MTS that are loaded with the Windows NT Client and/or Windows CE operating systems. The second area is that of the NA, located at the contractor facility and who is responsible for establishing security for the contractor provided UNIX Packet Switch.

The TFM is used to review skills and provide the system background necessary for administrative personnel to perform. It also suggests additional manuals along with reference and standardized materials needed by administrative personnel.

MTS is being developed in phases, based on the U.S. Army Training and Doctrine Command TRADOC operational requirements document (ORD), the MTS will follow a two-tiered incremental development strategy that will ultimately coincide with operational, environmental, and performance requirements as described in functional and technical documents for the system. The two phases of MTS development process are:

Block I is the initial operational capability (IOC). This version provides the core capability of a worldwide MTS with a system and architectural design that is stable, modular, scaleable, and easily upgradeable. This initial capability will be the baseline for follow-on enhancements.

Block II is the final operating capability (FOC). This version will deliver enhanced information flow, evolving capabilities, additional functionality, and interfaces to complete the system. The FOC will be achieved through the use of pre-planned product improvements (P3I), technology insertion, and technology additions.

Data processed by the MTS during Block I has been determined to be sensitive but unclassified (SBU). In normal operations, the data will not include privacy act related information. The data will include sensitive combat service support data and highly perishable location data of in transit logistical support vehicles. For Block II, the data within the system will be classified. MTS Block I will process data in “dedicated” mode. This is defined as processing, transmission, storage, or data that is within a single information category (All users and processes have been granted access to all processes and data, and all users have the same need-to-know). MTS Block II processing will take place in “System High” mode, requiring more severe security constraints. This will necessitate the full operation of a Trusted Computer Base (TCB). At Block II this guide will evolve into a Trusted Facility Manual.

A system security policy defines the relationship between the system users and the systemic processing and handling of data and information. Additionally, the security policy states the protection measures required to be implemented. The policy statements expand to a series of operational responsibilities that are managed in the system implementation. Some fundamental security policy statements are:

- **Accountability:** The property that enables activities on a system to be traced to the individual(s) and or processes originating the actions.
- **Availability:** The property that ensures system resources are available and usable to authorized processes.
- **Access Control:** The process of limiting access to the resources of a system only to authorized programs, processes, or other systems (in a network). Synonymous with controlled access and limited access.
- **Confidentiality:** The property that ensures data or information is accessible to only those users or processes possessing adequate authorization.
- **Integrity:** The property that ensures data or information has not been altered or destroyed in an unauthorized manner.
- **Non-repudiation:** The proof of delivery or origin of information transactions.

1.3. Document Organization

The TFM is organized as follows:

Section 1: Provides the purpose, scope and use of this TFM.

Section 2: Overview of the MTS architecture and boundaries including the hardware and software configurations for MTS.

Section 3: Physical and personnel security aspects, system threats, and threat countermeasures.

Section 4: Windows NT security architecture, screensaver access, logon process for the MTS, and Discretionary Access Controls (DAC).

Section 5: Discusses continuity of operation mechanisms for SAs such as backup and recovery, contingency planning, and logging into the MTS.

Section 6: Installation procedures for user accounts along with assignment of group accounts, user profiles, and home directories. This section also discusses the use of system auditing and event log procedures.

Section 7: Use of access controls for files, directories, printers, and the system registry. It also discusses the procedures for locking and logging off a workstation.

Section 8: This section discusses the installation process for MTS specific software and MTS Control Station or V2 software troubleshooting.

Section 9: Unix Security Architecture. Discusses the system backup and restore process for Unix along with the use of contingency planning.

Section 10: System configuration for IP Forwarding and the installation and configuration procedures for McAfee Anti-Virus software.

Section 11: Reviewing the concept of “least privilege” for assigning system permissions. This section also discusses DAC for setting UID and GID access.

Section 12: Files and directories on MTS that need to be assigned special permissions.

Section 13: This section talks about sharing and mounting file systems in relation to the MTS packet switch. This section also discusses user privileges within Unix based systems and provides two positions (DAA and IASO) in order to facilitate the process of security management.

Section 14: This section discusses local access accounts within MTS.

Section 15: MTS guidance regarding site-specific responsibilities and procedures.

Section 16: MTS countermeasure procedures for possible misuse.

Section 17: Discusses root and administrator account management.

Section 18: This section discusses audit requirements, policies, and analysis procedures within MTS.

Section 19: MTS utilizes DES encryption system when transmitting information via the transponders. This section explains the process for changing the DES Keys.

2. SYSTEM SECURITY OVERVIEW

2.1. Architecture Description

2.1.1. Hardware Configurations

The MTS system currently includes two distinct functional configurations: the Control Station (normally used in a fixed site), and the vehicle-mounted Mobile Unit (referred to as V2). The Control Station provides command functionality for the MTS, and is typically operated from a mobile headquarters, such as a command tent or a parked van. The Control Station operates independent of phone lines or Internet connections to coordinate vehicle movements using text messaging and theater maps displaying MTS-equipped vehicles to include the Control Station unit itself. It consists of a laptop computer with CD-ROM drive for National Imagery and Mapping Agency (NIMA) maps, a satellite transceiver with 100-foot-long cabling, and a portable color printer. More hardware details are available in Table 1.

The V2 mobile unit is designed for permanent installation in a vehicle using an installation kit designed for that vehicle. The kit consists of a satellite transceiver, ruggedized laptop computer, and appropriate cabling. The V2 mobile unit provides text messaging between vehicles in the group, and, using NIMA digital theater maps, a graphic display of deployed MTS-equipped vehicles including the V2 unit itself. More hardware details are available in the Table 1.

Table 1 MTS Hardware Configurations

Control Station	Computer	Ruggedized Laptop, Model 1100
	Processor	AMD K6-2, 400 MHz
	RAM	128 MB
	Hard Drive	Removable 2.5", 6 GB
	PCMCIA Reader	1 Type I/II 1 Type II/III
	CD-ROM Drive	20x
	Video	VGA
	COM Ports	2 RS-422 1 RS-232
V2	Computer	Ruggedized PGI, HHC
	Processor	5x86, 133 MHz
	RAM	64 MB

	Hard Drive	Removable 2.5", 2 GB
	PCMCIA Reader	1 Type I/II 1 Type II/III
	Video	VGA
	COM Ports	1 RS-422 1 RS-232

MTS Control Station standard configuration includes:

- One transceiver (MT 2010)
- One control box
- One power adapter connecting the control box to an AC power source
- One power/data cable connection from a connector on the MT 2010 to the control box
- One rechargeable battery pack inside the MT 2010
- One laptop computer
- One port expander
- One USB cable connection from the laptop to the port expander
- One RS422 cable connection from COM3 on the port expander to the RS422 port on the control box
- One power adapter connecting the laptop to an AC power source
- One laptop battery
- One portable color printer
- One data cable connection from the laptop's DB25 port to the printer
- One power adapter connecting the printer to an AC power source
- One printer battery

The Control Station can optionally include a precision lightweight GPS receiver (PLGR), enabling the unit to receive military-precision GPS. The optional components include one PLGR and one PLGR cable.

The V2 mobile unit's standard configuration includes the following components. Those followed by "A-KIT" in parentheses are included in the kit for permanent installation of the V2 unit. A-Kits are unique to each type of vehicle that the Army decides to equip with MTS. As of this time, the MTS system is approved for the following military vehicles: HMMWV, HET, PLS, FMTV and HEMMT.

-
- One mounting bracket for the MT 2010 (A-KIT)
 - One lanyard for the MT 2010 (A-KIT)
 - One mounting bracket for the laptop (A-KIT)
 - One MT2010
 - One control box (A-KIT)
 - One rechargeable battery pack inside the MT2010
 - One power/data cable connection from a connector on the MT2010 to the control box (A-KIT)
 - One laptop computer
 - One data cable connection from the COM2 port on the laptop to the RS422 port on the control box
 - One laptop battery
 - One power cable connection from the laptop to the power port on the control box

2.1.2. MTS Software Configurations

MTS software is based on an open system architecture running over the Windows operating system (OS), mapping software, and communications software. **MTS Messenger** is an application providing text message capability between the control stations and V2 mobile stations. It comes loaded and configured on the unit, and is activated when an authorized user completes the Windows logon process. **Tracerlink Tracking** is an application providing GPS tracking and automatic position reporting for the mobile units; **Tracerlink Mapping** interfaces automated tracking capability with on-board mapping software. **Tracerlink Tracking** and **Tracerlink Mapping** are pre-loaded and pre-configured; both programs are activated when an authorized user completes the Windows logon process on a V2 mobile unit or on a control station. Additional software is not authorized without written DAA approval and update of accreditation documentation. More software details are available in the Table 2.

Table 2 MTS Software System Configurations

Software	Control Station	V2
Windows NT 4.0, SP6	X	X
MTS Messenger	Version 1.38	Version 1.32
Tracerlink Pro Vehicle Tracking 2.0.3	X	X
Tracerlink Pro Mapping 2.0.3	X	X

McAfee Virus Scan (V 4.0.5 or later)	X	X
--------------------------------------	---	---

2.1.3. External Interfaces

No external interfaces will be allowed on MTS unless they have the explicit permission from the DAA. This permission will take the form of a letter of authorization and when the system is recertified, addition to the updated system security accreditation agreement (SSAA)

2.2. Accreditation Boundaries

As stated in Army Regulation (AR) 380-19, Paragraph 3.1e, accreditation addresses the system's perimeter, its boundary, and its relationship to other automated information systems (AIS) and networks within a particular infrastructure. The system perimeter surrounds the specified set of equipment and peripherals under the control of the DAA. The system boundary encompasses a larger environment that includes remote systems associated with the Gateway/Network Management Center separately accredited outside the system DAA's control. The system boundary may encompass numerous systems, users, organizations, and networks that support a similar mission objective. While the collection of all potential users of the AIS, that is, all users within the system boundary, are used to determine the security mode of operation of the system, only the AIS equipment and peripherals within the system perimeter of the AIS is specifically identified in the accreditation document as the accreditation boundary. The MTS system perimeter surrounds the specified set of equipment that is under the control of the MTS DAA.

2.3. Security Configuration

The MTS packet switch (PS) security configuration addresses the related elements that define the operating environment.

2.4. Packet Switch Controlled Environment Boundaries

The question of what is and what is not included, as part of a MTS PS facility for the purpose of C&A is not entirely answered by identification of the software that resides on the MTS PS host platforms and the identity of the acknowledged MTS PS host platforms themselves. The key determinant is whether or not an interface exists with a component in the MTS PS networked domain. If there is an interface, channel, or path between two components and one is an acknowledged MTS PS component, then both components must be considered in the MTS Packet Switch trusted facility C&A. The site DAA must be prepared to provide the protection required in accordance with MTS PS security policy.

2.5. Packet Switch Security Configuration Administration

The MTS Packet Switch security configuration details focus on the software elements that comprise the software version baseline:

- Platform OS files, directories, and system programs.

-
- Files, directories, and applications.
 - Mission critical system files, directories, software and database applications.

Establishing and maintaining the mission system security configuration is a process that is continually administered by the security staff. An established security configuration may change for valid reasons and therefore under the best circumstances the system's security configuration needs to be monitored and adjusted in response to operational needs.

2.6. Establishing the MTS Packet Switch Security Configuration

2.6.1. Snoop

The /bin/snoop command must be disabled for general use by maintaining permissions of 500 on the executable file.

3. SECURITY ENVIRONMENT

The MTS infrastructure, including all areas containing hardware components and associated cabling will be protected from unauthorized or inadvertent modification, misuse, or destruction. The MTS components shall be physically protected to the sensitivity level of information they contain or process when in operation. When not in operation, the terminals will be purged of all sensitive information and protected as any other high dollar equipment. The MTS infrastructure system management control and technical control facilities shall be properly protected to the appropriate level that the data processed requires. Personnel will use locking devices to physically secure resources during and after duty hours. This requirement applies to all workstations, terminals, and other MTS equipment. The MTS infrastructure, including all hardware and software components, and peripherals shall be appropriately protected for environmental conditions such as air conditioning, fire, heat, humidity, power quality and availability, dust and water damage. All mission data to, include messages, location information, maps, and application specific data, should be treated as mission sensitive and safeguarded in accordance with SBU sensitivity standards.

3.1. Philosophy of Protection

The security implementation is based on an approach to system security that emphasizes system security configuration and control, then, detection of aberrant activities. The system security staff will use the features provided by the operating systems and commercial/governmental off the shelf (COTS/GOTS) tool products to aid in the implementation and maintenance of the security configuration.

System Security configuration is based on the following tenets.

- Protecting and controlling Administrator or equivalent “super-user” type privilege is paramount.
- Controlling access to the interconnected system components begins with access point identity (i.e., network and communication connections and login methods) and applying the appropriate controls. Access control is maintained through pro-active and re-active configuration and audit trail monitoring.
- Ensuring only the approved file system objects and executable processes required to complete the operational mission are maintained on a system platform. No developmental tools will be maintained or available in the operational system environment.
- Auditing will be enabled for the approved audit events on all platforms.
- Ensuring unknown or unapproved file systems are never mounted in the operational system environment.
- File system security and integrity is ultimately and most effectively gained through sensible DAC and user privilege control (through user account and profiling control mechanisms) management.

-
- Preventing misuse will be accomplished through diligent security maintenance in support of these security tenets (i.e. the diligent examination of audit and security configuration compliance tool reports).
 - Database passwords will be unique to each individual user and applied to the internal and external authentication mechanisms as required. No external password will be operationally maintained for the purpose of over-riding internal database authentication controls
 - Establishment of a standard operating procedure (SOP) for each system site will consistently control the site-specific details of maintaining the system security configuration.

3.2. Threats to System Security

MTS information management personnel are concerned with threats that are carried by threat agents and have the potential to exploit system vulnerabilities which, in turn, may have a detrimental impact on the integrity, availability, and confidentiality of its IT resources. Generally, threat agents to MTS resources fall into the following four categories:

- Human
- Structural/environmental
- Natural disasters
- Technical

The following subsections describe and give examples of threat agents that fall into one of these categories.

3.2.1. Human

Human threat agents may be categorized as insiders, people who are authorized access to the MTS resources, or outsiders, people who are not authorized access to the MTS resources. Insider threats are characterized as accidental or malicious in intent. All outsider threats are considered to be of malicious intent. Human threat agents endanger all resource categories of a system: equipment, instruction, and other people. These threat agents are found outside the system (hackers, wiretappers, and other unauthorized personnel) and inside the system (users, SAs, information assurance security officers (IASO), managers, and other authorized personnel). Threats to equipment can include: destruction, theft, incorrect connection, or incorrect setup. Threats to instructions (including computer instructions) can include: incorrect program code, data modification, malicious code insertion to include viruses, code or data destruction, incorrect or obsolete standard operating procedures or other directives, incorrect operating instructions for computers, or incorrect equipment operation even though correct written instructions are available. Threats to other people may include blackmail, bribery, intimidation, or physical harm. (Another type of threat against the system in general is the threat of legal action taken as a result of the actions of an authorized user of the system. Data and software stored on the system may be subject to US Copyright Law, various licensing agreements, or the Privacy Act of 1974

as amended. Violation of these laws could cause the system to be legally shut down or, at least, a fine could be assessed against the agency.) Any of these threats can cause degradation in confidentiality, integrity, accessibility of the system and its data.

3.2.2. *Structural/environmental*

Structural/environmental threat agents are characterized as being either part of the environment or part of system equipment resources. Structural/environmental threats primarily endanger the system equipment resources, but, depending on severity and how quickly these agents act, people can also be harmed. These threat agents are found in the environment surrounding the system (fires, floods and extreme temperature variations within the building but outside the equipment rooms, utility pathways pipes, electrical conduits, ventilation ducts) within the equipment rooms or within the floors, ceilings or walls of the equipment rooms) or as part of the system (bare electrical wires, board-level components that are operating out of specified parameters, or weak raised floors). Equipment threats may include: disruption, temporary interruption, or permanent destruction of operation. Threats to instructions may include complete destruction. Threats to people may include loss of life. Together or separately, these threats may cause service denial for varying periods of time.

3.2.3. *Natural Disasters*

As threat agents, natural disasters are very similar to Structural/environmental threat agents. Both destroy the environment surrounding the system, and both exploit vulnerabilities that are difficult to lessen with even the best safeguards. With the distribution of MTS resources worldwide, the likelihood of the occurrence of a natural disaster affecting those resources is great. Natural disasters can affect all three kinds of resources in a system (i.e., equipment, instruction, and human) depending on distance and severity. Natural disasters that are not local or severe can still interrupt the communications channels upon which the system depends, thus causing degradation in the confidentiality, integrity, and accessibility of the system.

3.2.4. *Technical*

Technical threat agents are those deviations from system design specifications that impact system security. Hardware implants are examples of technical threat agents found in computer equipment. Small radio transmitters are sometimes found on memory boards that broadcast data outside authorized channels. Network components that are not thoroughly authenticated may not belong on the network and may be hijacking data. Technical threat agents found in a computer's software instructions may include programs that generate false logon screens; programs that store data in two locations, one of which is unauthorized; programs that destroy or modify data; or programs that allow incorrect processes, such as simultaneous writing to a file, to occur. Technical threat agents open unauthorized channels for data and cause service denial while the damage is corrected.

3.3. Physical Security Assumptions

The physical security requirements for the MTS are modest and are common to most other systems that transmit, store, or otherwise process sensitive-but-unclassified (SBU) information.

Although the degree of physical security may vary, physical security components will be used and measures will be implemented and maintained to include physical barriers and continuous monitoring of controlled areas; physical access controls; and components and/or measures for minimizing the impact of natural disasters. The MTS security policy requires that certain physical security controls be employed at each site because of the existing threats and vulnerabilities. Therefore, servers will be located within a secured perimeter protected by key lock, combination lock, cipher lock, or some type of security perimeter that controls individual access. Physical security controls must also be implemented by the SA to protect the PC terminals and to guarantee that only authorized personnel have unaccompanied access to the areas where these devices are located. In some cases, printers may be placed under physical controls to ensure that unauthorized personnel do not have access to data for which they have no need.

The operational site MTS IASO or SA determines the required physical security protection for MTS resources based on local risk assessments. These determinations will be ongoing throughout the system's lifecycle and are most important when local conditions change as a result of operations relocation, structural modification(s), unusual increases or decreases in the number of staff personnel, increased (or changes in) data sensitivity, etc. The following sections discuss the minimal protection that is recommended.

3.3.1. Surge Protection

Surge protectors or some other form of electrical power conditioning will be installed on all electrical power sources serving MTS resources to protect them from electrical damage.

3.3.2. Primary System Components Security

At a minimum, MTS hosts (V2 and Control Station) will be secured within a room(s) or vehicle that is routinely locked. Keys and/or combinations to each room/vehicle will be controlled so that unauthorized personnel cannot gain access to the components without taking unusual steps to gain entry.

Physical security controls are established to prevent unauthorized access to the MTS. To that end, the following protocols are provided:

- Protect information against inadvertent access by unauthorized persons.
- Use only approved containers or areas for media storage (i.e. printouts, removable media) when unattended.
- Double-check workstations/workspace prior to leaving them unattended or secured for the day, to ensure that all information is appropriately safeguarded. More than one set of eyes is best.
- Always log off computers or use a password-protected screen lock-out feature when leaving work area.
- Follow the MTS physical security policy/SSOP regarding workspace security

3.3.3. Secure Working Location

The general MTS work area will have at least the minimum level of physical security established to prevent theft of or tampering with MTS computer and telecommunication resources. Controlled entry and locked computer rooms are appropriate.

3.3.4. Secure Terminal Locations

If deemed necessary by the MTS IASO or SA, terminals will be placed to restrict personnel without a valid need-to-know from casually viewing data on the terminal screens.

3.3.5. Uninterruptible Power Supply (UPS)

UPS devices will be attached to MTS servers and on other associated primary computer resources that are necessary for the network to continue operation. The UPS will provide at least 10 minutes of emergency power support to permit the SA, to properly shut down the system without data loss. Additionally, as equipment acquisition permits, UPS devices must be capable of performing a proper emergency shutdown automatically.

3.3.6. Physical Security Standard Operating Procedures (SSOP)

SSOP regarding MTS physical security will be developed and distributed as widely as possible to ensure all MTS employees understand and comply with security measures in place to protect all MTS computer assets.

(Note: For natural and man-made disasters, and for technical threat contingencies, refer to the *MTS Contingency Plan*.)

3.4. Personnel Security Assumptions

It is a common mistake to assume since all users are cleared and that this negates the need for tight security. Since the MTS operates in the SBU Dedicated Security Mode, all users of the MTS must be cleared, have formal access approval, and a need-to-know for the highest level of data processed on the system. Therefore, all those with direct access to the MTS must, at a minimum, occupy positions designated automated data processing (ADP) level 2. Maintenance personnel who do not access classified data during their maintenance operation must, nevertheless, be cleared for the highest level of data processed on the system. However, if this is not feasible, maintenance personnel will be monitored at all times during their maintenance operation by individuals with the technical expertise to detect unauthorized modifications.

3.5. Personnel Security Training and Awareness

Users must receive security awareness training before they are given access to the MTS, and regularly scheduled, refresher training thereafter. Listed below are topics each user must understand, most of which are covered in this guide. If a user does not understand any of these topics, it is in their best interest to contact their IASO.

-
- *Threats, vulnerabilities, and risks associated with the system* - Users must get specific information regarding measures to reduce the threat from malicious software including prohibitions on loading unauthorized software, the need for frequent backup, and the requirement to report abnormal program or system behavior immediately.
 - *Information security objectives* (i.e., What is it that needs to be protected?)
 - *Responsibilities and accountability associated with network and computer security*
 - *Information accessibility, handling, and storage considerations*
 - *Physical and environmental considerations necessary to protect systems*
 - *System data and access controls*
 - *Emergency and disaster plans*
 - *Authorized systems configuration and associated configuration management requirements*

Periodic security training and awareness may include various combinations of the following:

- Self paced or formal instruction
- Security information bulletins
- Security posters
- Training films and tapes
- Computer-aided instruction

Refer to the MTS security awareness training & education (SATE) plan for more information.

3.6. System Security Countermeasures

MTS is subject to the same range of generic threats applicable to any government information systems processing SBU information. A potential threat exists to the confidentiality, integrity, and accessibility of the information processed, stored, and transmitted by the system. Potential threats to the MTS come from natural and manmade sources. Natural disasters and damage can result from fire, water, wind, and electrical sources. Man-made threats are from those who would target MTS for espionage, criminal activity, unlawful use, denial of service, or malicious harm. External or internal agents of threats include espionage services, terrorist, hackers, and vandals.

Statistical analysis of computer-related incidents used to indicate the greatest threat to MTS would be from a trusted agent who has access to the system. The current model shows internal and external threats nearly even. The most likely internal incident involves an authorized user who accidentally or inadvertently commits or omits some action that damages or compromises the system, one of its components, or information processed, stored, or transmitted by the system. The next most likely incident involves an authorized user who takes deliberate action to damage the system, one of its components, or its data for personal gain or vengeful reasons. Such a person could also engage in espionage, other criminal activity, or exploitation or expropriation of the assets of the system for personal gain. There is the threat of the co-option of users with

authorized access to the system, or contractor support personnel, with physical access to the system components arising from the motivation of financial gain. Then there is the threat posed by disgruntled employees, especially those who are to be terminated for cause. Also there is a threat posed by users of the system who negligently or inadvertently fail to follow security requirements for the handling and labeling of system output or media, or the rules against the introduction of unauthorized software or data. Finally, there is the threat arising from the failure of authorized users to employ proper procedures for the entry or manipulation of system data due to failure of users to be properly trained in the use and operation of the system.

- These insider threats can be manifested in the following ways:
- The unauthorized reading, copying or disclosure of sensitive information
- The execution of denial of services attacks
- The introduction into the system of viruses, worms or other malicious software
- The destruction or corruption of data (intentional or unintentional)
- The exposure of sensitive data to compromise through the improper labeling or handling of printed output
- The improper labeling or handling of magnetic media that would result in the compromise of sensitive information

The co-opted insider would most likely copy to disk and remove from the system any and all types of sensitive information to which such user had authorized access. Such a user might also probe the system in an attempt to discover ways to circumvent access permissions, copy and remove from the system sensitive information to which such a user did not have authorized access. This might be attempted by an extremely sophisticated user or hacker (or by someone that is under the direction and control of such a person). The individual might be attempting to discover ways to introduce a software sniffer into the system to learn the user ID and password of a system administrator or other privileged user, and, by masquerading as such a user, bypass access controls and gain access to the most sensitive information on the system. In instances of these types of attacks, there could well be attempts to gain unauthorized access to and modify audit data in order to prevent analysis and detection of the source and nature of the attack. It goes without saying, that the most serious of all types of possible attacks against the system could be mounted by co-opted systems administration personnel, with their ability to alter or bypass most, if not all, of the system's protection mechanisms.

3.7. Policy Based Countermeasures

Security Countermeasure development requires two areas of focus due to the unique design of the MTS, the first area is the Windows NT environment of the mobile/portable terminals, and the second area is the UNIX environment of the MTS packet switch.

3.8. Copyright Laws

Personnel who violate copyright laws will be subject to disciplinary actions per appropriate Army regulations, which may result in civil or criminal penalties by judicial actions. U.S. Army Copyright Policy is noted in the AR 380-19 paragraph 2-3a(12).

3.9. Hard and Soft Copy Markings

Hard and soft copy output is required to be treated and handled in accordance with system classification guidelines. Soft copy output is defined as any data that has been saved to a CD ROM or Floppy Drive and Hard copy output is defined as data that is printed on a printer. All of these outputs can only be done via the Control Station and must be posted at the highest level of security for the data that is contained within MTS.

Data to be processed by the MTS has been determined to be Sensitive But Unclassified (SBU) and all outputs are set as For Official Use Only (FOUO). In normal operations the data will not include information covered by the privacy act. The data will include sensitive combat service support data and highly perishable location data of in transit logistical support vehicles

4. SECURITY ARCHITECTURE

4.1. Windows NT Security Architecture

Windows NT Workstation features an integrated security architecture consisting of several components, including:

- Security Reference Monitor
- Local Security Authority
- Security Account Manager
- Mandatory, Secure Logon Process

The overall system architecture is divided into two main areas: the kernel mode and user mode. Within this architecture, Windows NT is able to apply security to the objects and processes within its control.

4.2. Security Reference Monitor

The Security Reference Monitor (SRM) is part of the Windows NT Executive within the kernel. It is responsible for enforcing all access validation and audit policies defined within the Local Security Authority. In this way, the SRM is designed to protect all system objects from unauthorized access or modification. This ensures that all protection is provided uniformly to objects on the system. The SRM provides services for validating access to objects, generating audit messages that are subsequently logged by the Local Security Authority, and verifying user accounts for the appropriate privileges.

4.3. Local Security Authority

The Local Security Authority (LSA) provides many services to the security subsystem of the Windows NT operating system. It is designed to ensure that the user has permission to access the system by validating the user during logon. It manages the local security policy as set by the administrator, generates access tokens, and provides interactive validation services when access is requested for any system object. The LSA also controls the audit policy, set by the administrator, and writes any messages generated by the Security Reference Monitor to the event logs.

4.4. Security Accounts Manager

The Security Accounts Manager (SAM) controls and maintains the Security Account Database. The security account database contains account information for all user and group accounts. The SAM provides the user validation service during logon that is used by the LSA. During logon, a cryptographic hash of the password entered is compared with the hashed password stored in the security account database. If this comparison is successful, the user's Security Identifier (SID), as well as the SIDs for any groups the user belongs to, is provided back to the LSA for the creation of the access token that will be used during that session.

4.5. DoD Security Banner

All computer systems that are connected to the DoD network must contain a warning banner that identifies the system as a DoD System and that once a user logs onto the system you will be monitored for security purposes. The text that is contained within the DoD Banner is noted below.

Department of Defense Warning Banner

Attention:

This is a DoD computer system. Before processing classified information, check the security accreditation level of this system. Do not process, store, or transmit information classified above the accreditation level of this system. This computer system, including all related equipment, networks, and network device (includes internet access) are provided only for authorized U.S. Government use. DoD computer systems may be monitored for all lawful purposes, including ensuring their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes, but is not limited to, active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring. Unauthorized use of this DoD computer system may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for all lawful purposes.

4.6. Logon Process

The Windows NT logon process is mandatory for initiating a session. The logon is a multi-step process:

- Enter User-Id and Password
- The password is hashed and sent to the Local Security Authority.
- The LSA makes a call to the authentication package and compares the hash to the hash stored in the local SAM database
- The LSA creates an access token using the information returned from the authentication package
- The NT Explorer Shell opens with the user's access token attached

4.7. Screen Saver Access

Windows NT allows the use of a screensaver that will control user access to the workstation when left idle for a specific amount of time. Although this feature allows for

the compliance with AR 380-19 para 2-11c(3) and 2-11c(4), the DAA has determined that this feature need not be pre-activated and should only be used when not hindering the ability of user to properly access the system. The screensaver will utilize the MTS user accounts within Windows NT and will require a valid userid and password to re-obtain access to the system.

Upon the system being in locked mode, only the current user or a user with administrative privileges will be able to regain access. The screensaver will be set to activate upon being idle for 3 to 5 minutes.

4.8. Discretionary Access Controls

At the dedicated SBU mode of operation, Discretionary access controls are not required. However, they are resident in the Windows NT Architecture, and can provide the Systems administrator options for ensuring adequate security within MTS. Discretionary Access Controls (DAC) provide object owners the means to control who can access resources as well as the type of access they may have. Access to system resources, such as files, directories, printers, and network shares, can be controlled either through GUI-based system tools or through the command line.

Objects in Windows NT support discretionary access controls. The NT Explorer, Print Manager, and Registry Editor are tools provided with Windows NT that can be used to manipulate DAC's on the common objects that users and administrators work with in the Windows NT environment.

4.9. Access Tokens and Security Identifiers (SID)

The Local Security Authority creates access tokens after SAM validation as part of a successful logon process. The access token created at that time is associated with the user's session for the lifetime of the session. Whenever a user initiates a process during the course of the session, a copy of the token is attached to that process. Once the user logs off, the token is destroyed. Each token contains the following information:

User's Security Identifier (SID)

- Group Security Identifiers for the groups to which the user belongs
- User privileges
- Owner SID (assigned to any objects created during the session)
- Primary Group SID
- Default ACL (assigned to any object created by the user)

5. PROTECTIVE MECHANISM FOR SYSTEM ADMINISTRATORS

5.1. Logging onto MTS

MTS uses Windows NT 4.0 as its operating system (OS). The OS will authenticate each user and will allow them to have certain privileges within MTS. Each user will have to maintain the security of their user account by not writing down their account information or giving their information to another user. The user accounts have strict password policies and guidelines. These policies and guidelines are noted below in section 5.1.1 - 5.1.2.

5.1.1. Password Policy

NOTE: Passwords are case sensitive. The SCI manufactured V2 computer, there is no CAPS Lock indicator light.

All passwords will:

- Be at least eight characters in length
- Contain special characters (ex. %*@), at least two numeric characters (1, 2, 3, etc.), and upper/lower case alpha characters (Aa, Bb, Cc, etc)

5.1.2. Password Guidelines

MTS also has certain guidelines for passwords. They are listed below:

- Not be a password that was used within the previous ten password changes
- The alpha characters must not be a word found in a dictionary or a name that can be spelled forwards or backwards
- Not be a simple keyboard sequence, such as asdfghjkl, or repetitions of the user ID (e.g., user ID is ann; password is annann)
- Passwords will expire 180 days after the computer is initially started at the factory for all users
- Users will receive a notification 15 days prior to password expiration
- Only a System Administrator can set up a users initial password. Standard users cannot change their own passwords until the previous password expires
- Three consecutive incorrect password attempts within 30 minutes will lock out each user until a System Administrator re-enables the user
- Password history is maintained. The operating system remembers the last 10 passwords
- Passwords must be changed semi-annually

5.1.3. Password Lifetime

Password lifetime (also known as password aging) refers to how long a password is valid on the system. For the MTS Packet Switch, the maximum lifetime of a password on the system is 180 days. A recommended minimum password lifetime is 15 days. Some users have a “favorite” password and by establishing a minimum password lifetime it ensures that users do not change their password three times in a short period of time (i.e., a few minutes, hours, several days) with the last change back to the original one. If quick successive changes are allowed, it ultimately circumvents the password history rule by allowing users to keep the same password. In 15 days, the user will probably remember his/her password and may not desire to change it for the sake of familiarity with the original one.

5.1.4. Root/Administration/Super-User Password Management

Because having the root privilege allows total system access, information for every user who is given the root password must be maintained in a Password Log. Information such as name, phone number, address, dates given the password, and clearance level must be entered for each person.

Additionally, maintenance personnel who have access must be maintained in this root password log. They must be monitored while they are performing maintenance functions. When maintenance personnel have completed the designated tasks, the password must be changed within minutes of their completion.

The security manager and the security staff have a responsibility for security of the system. Therefore, in order to perform their duties, they must be allowed root access to the systems for which they are responsible. They may not need root access in the daily routine tasks, but they may have to quickly respond to a situation that requires root access. Time limitations, on-going system activity, or unavailability of personnel with root access may prevent them from obtaining root access at the time which they actually need access.

All users who have access to the administrative roles must have a normal user account. These users must use the normal user account for the routine operations. When it is required to perform a privileged operation, the user must use the su command to modify their effective user ID to the system to gain privileged access. With the exception of emergency or contingency situations, all users are required to log on to the system using their normal user account.

5.1.5. Passwords and Shadow Files

The password file must maintain read permissions to allow interfacing with the applications. The shadow file must be maintained with zero access at the group- and world- levels.

5.2. System Backup, Recovery, and Contingency

5.2.1. System Backup

At this time, there is no need to backup mobile/portable terminals using Windows NT. MTS data is perishable by nature; therefore, the V2 and Control Station will recover system files (OS, mapping software, etc) in the form of a standard maintenance action. Archiving of audit logs will be addressed in the audit section of this manual.

5.3. Contingency Planning

The site contingency plan is usually activated under abnormal circumstances when system and/or environmental activities prevent continuing system operations at the site (i.e., natural disasters, and civil disruptions). Some issues that need to be addressed for contingency operations:

- Ensure there is a current site Contingency Plan
- Ensure there is a Memorandum of Agreement (MOU) with the contingency site
- Ensure operational equipment exists at the backup site
- Ensure necessary supplies exist at the contingency site
- Regularly brief all personnel on the contingency plan (causes for activation, personnel roles and responsibilities, points of contact, contingency site location, etc.)
- All recovery disks and system backups are not to be located in the same locations and must be able to go to the contingency site

5.4. Security Configuration

The security configuration addresses the related system elements that define the operating environment:

- The version baseline
- The network environment and relationship between platforms of the system.
- The configuration details of the platform OS's

5.5. Controlled Operating Environment

The MTS Windows NT OS consists of the kernel, infrastructure services, and common support applications. Each component is controlled through release and version tracking nomenclature that identifies the elements making up the component. The security staff will be most concerned and involved with the software control.

5.6. Software Version Baseline Control

The version baseline software is composed of software that provides the fundamental mission functions. These functions are the superset of the total software set and have

undergone a series of development, integration, security, and operational testing before fielding by a Configuration Management process.

The software version control is exercised through the MTS Program Manager Configuration Management Staff. Before being entered into the configuration management library, each software version change and its associated documentation is reviewed for completeness, integration tested, functionally tested, security tested, and then cataloged in the configuration management library for distribution.

5.7. Site Mission-Specific Software Control

The version baseline software contains the components (kernel, infrastructure support applications and common support applications) that are likely to be required at any given facility. In conjunction with the version baseline software, there are additional software components that are required for site-specific mission applications at some facilities. Although not part of the version baseline software, mission-specific software may be integration tested by the MTS Program Manager if it is to become a Configuration Management Item within the system.

5.8. Controlled Environment Boundaries

The question of what is and what is not included, as part of a facility for the purpose of C&A is not entirely answered by identification of the software that resides on the host platforms and the identity of the acknowledged host platforms themselves. A key determinant is whether or not an interface exists with a component in the networked domain. If there is an interface, channel, or path between two components and one is an acknowledged component, then both components must be considered in the C&A. The site DAA must be prepared to provide the protection required in accordance with the security policy.

5.9. Security Configuration Administration

The security configuration details focus on the software elements that comprise the software version baseline, such as:

- Platform OS files, directories, and system programs
- Files, directories, and applications
- Mission system files, directories, software and database applications

Establishing and maintaining the mission system security configuration is a process that is continually administered by the security staff. An established security configuration may change for valid reasons and therefore under the best circumstances the system's security configuration needs to be monitored and adjusted in response to operational needs.

5.9.1. IAVA Protect Tools – C2 Tools

The use of C2 tools are not required by the DAA, but the SA or IASO will utilize the Information Assurance Vulnerability Assessment (IAVA) Protect Tools (C2 Tools) found

FOR OFFICIAL USE ONLY

on the DISC4 homepage to review system security on MTS as needed. The IAVA tools are used to examine the security of a system for possible vulnerabilities. The tools also allow detailed examination of specific system users.

The ability to examine user areas is not allowed unless the SA or IASO gets prior approval from the Site Chief or Commander. This will only be done when a user has committed a security violation and an investigation is warranted.

5.9.2. Password Complexity Tool – C2 Tools

One of the C2 Tools called the Password Complexity Tool is used to enforce password policy and guidelines within the MTS. Completing the following commands can start this tool:

- Click on the **Start button**, select **Programs**, and select **Command Prompt**
- At the prompt “C:/" type in <passprop/complex>
- At the prompt “C:/" type in <noadminlockout>
- At the prompt “C:/" type <exit> to close the open window

5.10. McAfee Anti-Virus Software

In this time and age, information systems have to be protected against computer viruses, some of which can delete data or even make operating systems unusable. MTS is currently configured with McAfee Anti-Virus for both Unix and Windows NT 4.0 (Control Station and V2). These software configurations are shown in section 10.3 of this document.

Upon detection of a possible virus, the SA will contact the MTS IASO who will in turn notify the Site Chief or Commander. The IASO will then contact IAVA via the DISC4 homepage noted below:

- <http://www.disa.mil/> (INTERNET)
- <http://iase.disa.mil/> (NIPRNET)
- Cassie.iiie.disa.smil.mil (SIPRNET)

A MTS user must follow the chain of command upon detection of a virus. They will not be allowed to contact IAVA directly and must contact the MTS SA immediately upon discovery of the virus.

6. SYSTEM INSTALLATION FOR WINDOWS NT 4.0

This section of the TFM contains specific information on how to install and configure the system securely and for managing user accounts and ensuring enforcement of user related security policies.

6.1. Accountability

This section discusses the procedures for installing and securely configuring Windows NT 4.0. It also provides established procedures for managing user accounts and ensuring enforcement of user related security policies.

6.1.1. Windows NT 4.0

Installation and configuration of the Microsoft Windows NT operating system for the MTS components will be completed in accordance with the guidelines provide by the *Guide to Implementing Windows NT in Secure Network Environments*, Version 1.1, (referred to as the NT STIG in this TFM), and *Security Tips for WINDOWS NT 4.0 SERVER with Service Pack 6*. If not already done so, the optional Resource Kit for Windows NT 4.0 will be purchased, installed, and configured according to C2 level.

6.1.1.1 Userid and password

Although counter to DISA/DA policy, only two generic userids will be configured for each system. The userid for system operators will be “mts” while the userid for system administrators will be “cssamo.” Each will be configured with a preset password set to expire after 90 days. A third userid will be reserved for vendor technicians. The guest account will be disabled.

6.1.1.2 Additional configuration points

- The “passfilt” dynamic link library will be installed and enabled to enforce “strong” passwords.
<http://support.microsoft.com/support/kb/articles/q161/9/90.asp>
- Set antivirus software (Norton/McAfee) to automatically scan all drives connected to the system. Update virus definition files on the Control Station on bi-weekly basis. Update virus definition files on V2 when new software is introduced to the system.
- When prompted for inclusion of OS/2 options, select “no.” If the system is being configured after the fact (existing install), navigate to (find: files and computers) and remove the following files: OS2.exe, OS2SS.exe, OS2.SRV.exe, and OS2. Removal of these will negate vulnerabilities associated with their function.
- After installation of the operating system, navigate to (find: files and computers), and remove the following files: POSIX.exe, PSXDLL.dll, and PSXSS.exe. Removal of these files will negate vulnerabilities associated with their function.
- Compare audit settings to those found in the NT STIG and verify compliance.
- CD autorun must be disabled in all non-administrative userids

- Windows NT 4.0 is not C2 compliant when networked, but it can be configured to provide a maximum level of security when networked to other platforms. The Resource Kit allows the administrator to configure Windows NT for C2 mode.

6.1.2. Post-Service Pack 6 Hot-fixes for Windows NT 4.0

Windows NT 4.0 requires installation of Service Packs that fix security problems and general errors that arise after it has been put into service. The current Service Pack is called Service Pack 6 (SP6) and its installation is explained in section 6.1.1 of this TFM.

Windows NT will also utilize “hot-fixes”. Hot-fixes are basically like Service Packs but that they are created when an error or security problem is deemed a priority.

The U.S. Army issued a memorandum called *ACERT/CC Information Assurance/Vulnerability Alert (LAVA) Compliance Message 99-031, Securing Windows NT 4.0 Server/Workstation*. The memorandum explains how to securely configure Windows NT using Service Pack 6. It identifies the hot-fixes that are deemed necessary, where to download the fixes, and how to install them. The memorandum is located at the following web address:

<https://akocomm.us.army.mil/c2p/nsip/iapol/messages/042100zmar99.htm>

This process, the installation of service packs and hot fixes, will be kept up to date and documented.

6.1.3. User Accounts

The MTS is pre-configured with generic userids for both operators and administrators. If the need arises, the following procedures will be used to manage user accounts. The User Manager is the starting point for managing user accounts and establishing user related security policy. To display the User Manager dialog box) click on **Start**, click on **Programs**, click on **Administrative Tools**, and then click on **User Manager**.

A user account consists of all the information that defines a user to Windows NT. This includes the user name and password, groups in which the user group has membership, and the rights and permissions the user has for using the system and accessing its resources. Creating new user accounts is demonstrated below.

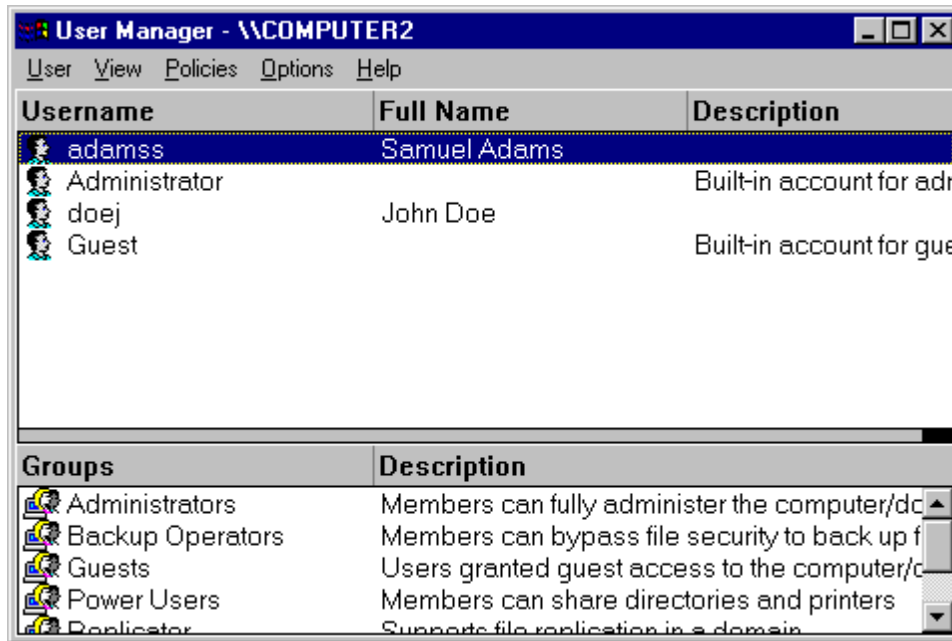


Figure 1 User Manger

6.1.4. Account Policy

Before creating any new user accounts, the security staff must establish the overall policies on how accounts will be configured. These account policies apply to all users within the system or domain and can be specified using the following steps.

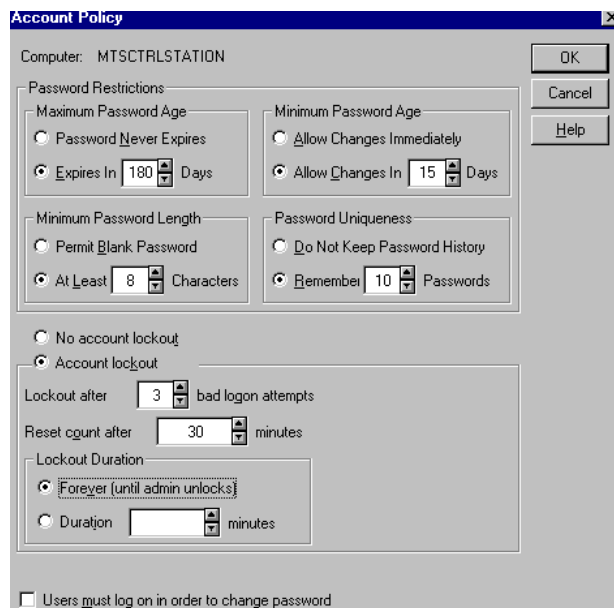


Figure 2 Account Policy

FOR OFFICIAL USE ONLY

- Starting with the User Manager dialog box, Click **Account** on the Policies menu to bring up the **Account Policy** dialog box
- Select **Expires In [180] Days under Maximum Password Age**
- Select **Allow Changes In [15] Days under Minimum Password Age**
- Select **At Least [8] Characters under Minimum Password Length**
- Select **Remember [10] Passwords under Password Uniqueness**
- Select **Account lockout**
- Select **Lockout after [3] bad logon attempts area**
- Select **Reset count after [30] minute's area**
- Select **Forever (until admin unlocks) under the Lockout Duration area**
- Click on the **OK** button to finalize Account Policy settings

Recommended settings for the Account Policy can be found in the *Defense Information Infrastructure (DII) Common Operating Environment () Secure Windows NT Installation and Configuration Guide*.

6.1.5. Creating a New User Account

To create a new user account, use the following procedure.

- From the User Manager dialog box, select **New User** from the **User** Menu to bring up the New User dialog box

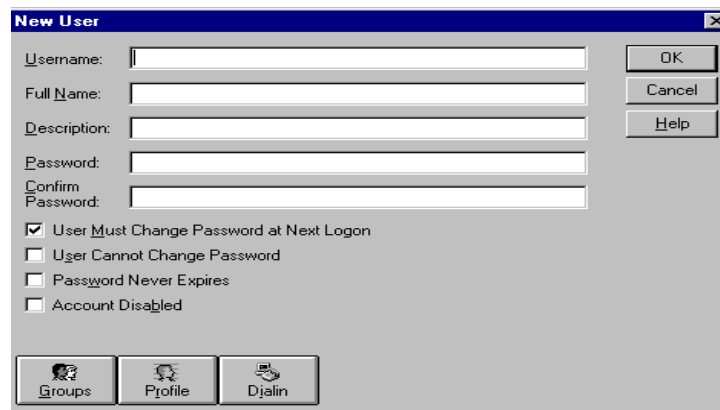


Figure 3 New User Dialog Box

- Enter the **username** for the new account. The next two fields, **Full Name** and **Description** are not required, but recommended to facilitate user management.
- Enter Password and Confirm Password
- Check the box for **User Must Change Password at Next Logon** (assuming the user, rather than the administrator is to choose passwords). If operating

FOR OFFICIAL USE ONLY

procedures require administrators to assign passwords, check **User Cannot Change Password**

- **Password Never Expires** must not be checked
- **Account Disabled** would normally not be checked (except, in the case of the Guest account)
- Select the **Groups** button to specify groups in which the user account is to be a member

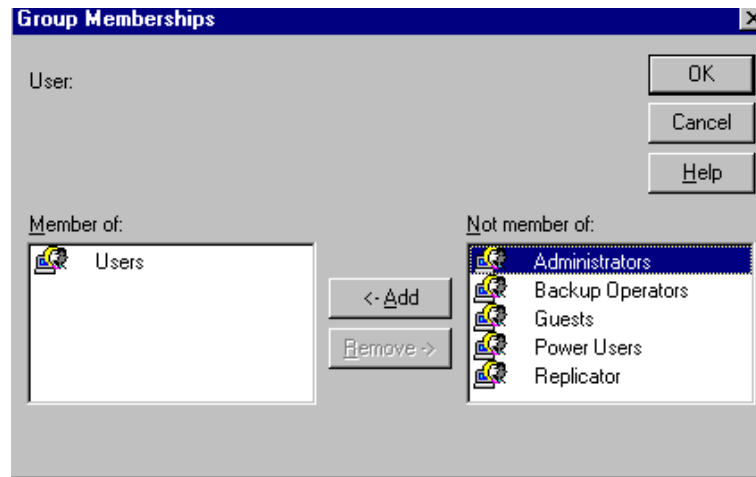


Figure 4 Group Memberships

- Select the **Profile** button to specify a user profile. This button allows the administrator to set up the user's personal profile, logon script, or home directory, and drives to connect on logon (see User Profiles Section)

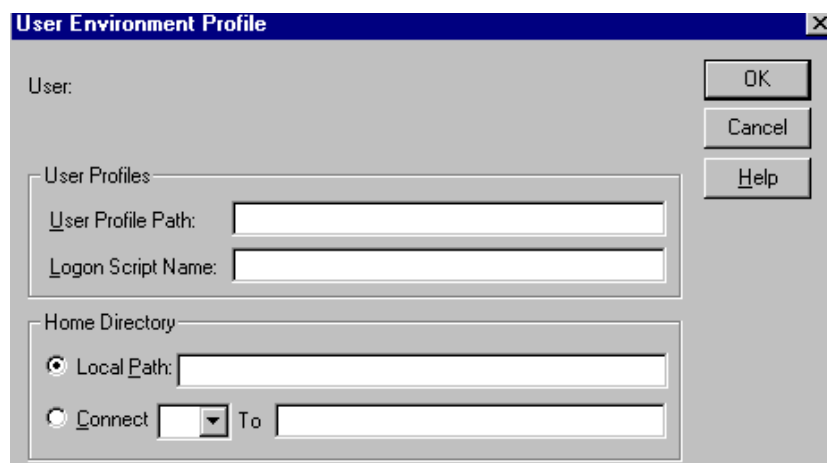


Figure 5 User Profile

- Select the **Hours** button to specify the hours during which the user account can connect to the system. Windows NT does not allow primary or secondary logons

during prohibited hours and the domain controller can be instructed to cancel remote user sessions

- Select the **Logon To** button to specify the workstations from which the user can log on. The default allows access from any workstation in the domain
- Select the **Account** button to manage the account expiration date and whether this is a global or a local account
- Select the **Dial in** button to specify whether this account can be used for remote access services

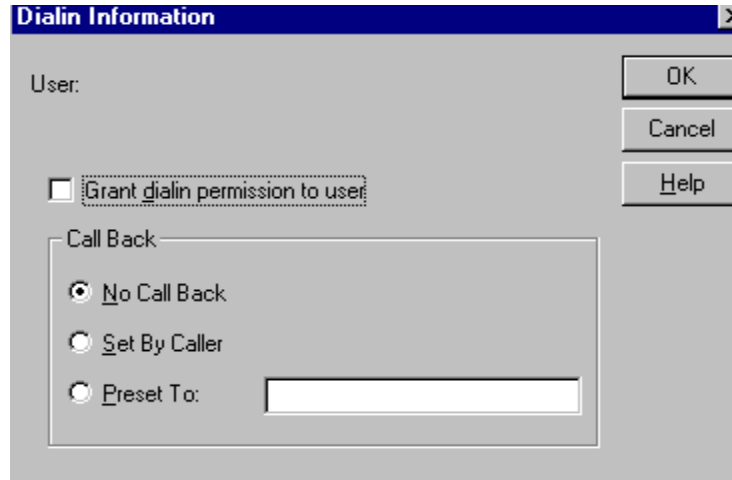


Figure 6 Domain Information

6.1.6. Built-In Accounts

By default, Windows NT creates two built-in accounts when installed: the System account and the Guest account.

The **System account** is an internal account, not a user account. It does not show up as an account in the User Manager, cannot be added to any groups, and cannot have its rights changed. It is an account that the operating system uses to run programs, utilities and device drivers. It does, however, have unlimited privileges. Therefore, if a Trojan horse program were able to infiltrate a system and run under the System account it would have the ability to do unlimited damage to the system.

Administrators must be very careful when installing services and running them under the System account. Some services (such as Server and Workstation) will only run under the System account, however, un-trusted services must never be allowed to run with System privileges. They must be run under a special account with the lowest level of access rights and permissions required for that service to run.

The **Guest account** allows people to access a Windows NT computer without logging in to a specific account. **The Guest account is disabled by default on Windows NT 4.0. The security policy guidance recommends that the Guest account remain disabled.**

6.1.7. Groups

Groups provide a convenient way to group together users with some common attribute or affiliation (such as all of the database administrators (DBA) group can be added to a DBA account group). Access to resources can then be granted to the group as opposed to having to specify each user by name.

- To create a new group, select **New Local Group** from the User Manager's **User** menu or select either **New Local Group**. Enter a name for the group and, optionally, a group description. Add users to the group by selecting the Add button, which will bring up a window of user and group accounts defined on the local system
- Group membership can be altered later by selecting the group name in the User Manager and selecting **Properties** from the **User** menu (or by double-clicking on the **group name**)

Windows NT defines two types of groups: local groups and global groups. Local groups exist only in the context of the local machine and can contain local user accounts, domain user accounts, and global groups. Global groups exist within the context of the domain. Global Groups are not used within MTS.



Figure 7 Local Groups

6.1.8. Built-In Groups

By default, Windows NT creates several built-in groups. These built-in groups are described in Table 3 below:

Table 3 Built-In Groups

Group Name	Description
Administrators	This group exists on all Windows NT workstations and

FOR OFFICIAL USE ONLY

	<p>represents the most privileged authority in Windows NT. They have all rights granted to them, or the ability to grant them to themselves.</p> <p>They do not, by default, have explicit access to all files and directories, but can take ownership on any file or directory and then grant themselves access. It is through membership in this group that the Administrator account is granted privileges.</p>
Backup Operators	<p>This group exists on all Windows NT workstations and servers. Users in this group are able to backup and restore (and, therefore, read and write) any file in the system, regardless of the ACLs on those files.</p> <p>No users are placed in this group by default.</p>
Domain Admins	<p>This group exists only on Windows NT servers acting as primary or backup domain controllers.</p> <p>By default, whenever a computer is added to a domain, the Domain Admins group is added to the local Administrators group. Therefore, members of this group have the ability to administer any computer in the domain.</p> <p>By default, the Domain Admins group includes the Administrator account for the domain controller.</p>
Domain Users	<p>This group exists only on Windows NT servers acting as primary or backup domain controllers.</p> <p>Members of this group have the right to log onto a system across the network.</p>
Guests	<p>This group exists on all Windows NT workstations.</p> <p>Members of this group can log on locally to a workstation.</p> <p>By default, the Guest account is a member of this group.</p>
Power Users	<p>This group exists on Windows NT workstations..</p> <p>In addition to the rights granted to Users, members of this group are permitted to manage user accounts that they create. They can also create, delete, and modify shares for both directories and printers, and are able to add/remove users from the Power Users, Users, and Guests groups.</p> <p>By default, no user accounts are placed in this group.</p>
Replicator	<p>By default, this group exists on all Windows NT workstations.</p> <p>Members of this group can replicate files within</p>

FOR OFFICIAL USE ONLY

	directories to other authorized systems. To do so, members of this group are given the right to log on as a service. By default, no user accounts are placed in this group.
Users	The Users group exists on all Windows NT workstations Members of the Users group can: <ul style="list-style-type: none">- Log on locally; Maintain a local profile; Lock the workstation; Shutdown the workstation; and Create/delete local groups on that workstation.

Specific recommendations for memberships in these groups can be found in the Defense Information Infrastructure (DII) Common Operating Environment () Secure Windows NT Installation and Configuration Guide.

Other groups are created automatically by the system on setup but do not show up in the User Manager. These groups, referred to as system or special groups, are described in Table 4.

Table 4 System Groups

Group Name	Description
Interactive	This group includes all users who log onto a Windows NT computer locally
Creator/Owner	This group is created for each sharable resource in a Windows NT computer. Its membership includes the users who either create a resource (such as a file) and those that have taken ownership of a resource.
Everyone	This group includes all users who can access a Windows NT computer. It is not possible to create a user who is not a member of the Everyone group.

6.1.9. Assigning User Profiles, Logon Scripts and Home Directories

As indicated in the previous section, the administrator can set up the user's personal profile. In Windows NT, different customizable profiles are automatically created for

FOR OFFICIAL USE ONLY

each user who logs on to the computer. User profiles can be local and mandatory. Local profiles are local to the computer on which they are created. The user can alter local profiles during their logon session. These changes will be saved upon logout and will be visible next time the user logs onto the system.

For Mandatory profiles, the user can modify their desktop during any logon sessions, those changes will not be saved for the next session.

Table 5 User Profile Settings

NT Object	Description
Control Panel	The user profile contains all user-definable settings for those control panel applications that support end-user configuration such as the mouse, screen colors, cursors, sound, and international settings. In addition, the profile stores all user environment settings.
DOS Command Prompt	The user profile contains all user-definable settings for the DOS command prompt including buffer settings, fonts, and colors.
File Manager	The user profile contains all user-definable settings such as network drive mappings.
Help System Bookmarks	The user profile contains all bookmarks that the user places in the Windows NT help system.
Print Manager	The user profile contains all the user's settings in the Print Manager, including network printer connections.
Program Manager	The user profile contains all of the user-definable settings including personal program groups and icon layout.
Third-Party Applications	The profile may contain information about third-party applications if these applications support the use of profiles.

Custom profiles can be assigned to individual users via the User Manager. To create a custom profile and assign it to a user or users, use the following procedures:

- Log on to a Windows NT computer under a generic user account and configure the environment to match the desired profile settings
- Log off the computer and log back in as Administrator (or other appropriately privileged account name)
- Open the **Control Panel**, double click on the **System** icon and select the **User Profiles** tab. You will see a list of available profiles (identified by the account name under which they were created)
- Select the profile that was created in the first step and click on the **Copy To** button

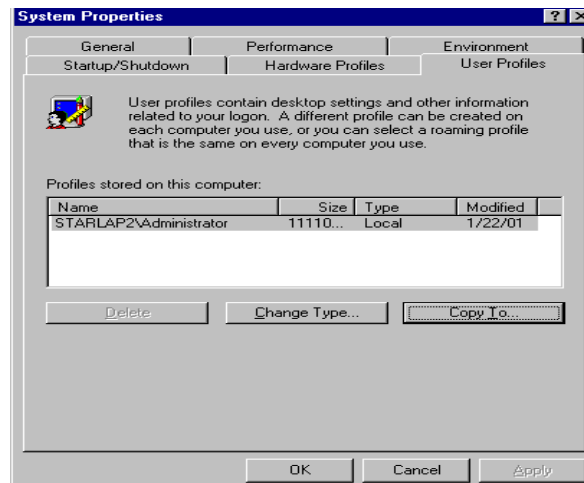


Figure 8 Profiles

- Click on the Browse button to select the desired location to where the profile will be copied
- Click on the Change button to alter the list of users who will be permitted to use this profile
- Click on the OK button when finished

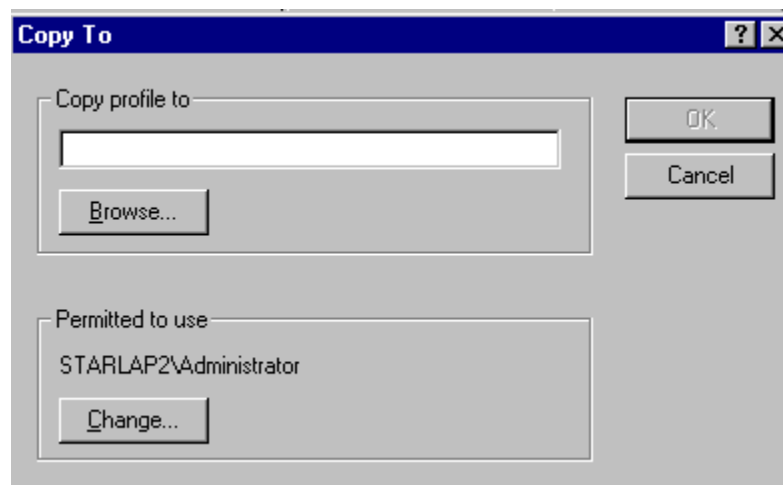


Figure 9 Copy To

- From the User Manager tool, either select **New User** from the User menu or **double-click on the name of an existing user** (depending on whether you are creating a new user or assigning a profile to an existing user)
- Bring up the **User Environment Profile** dialog box by clicking on the **Profile** button in the **New User** or **User Properties** window
- Enter the path to the profile created in the previous step in the User Profile Path text box

FOR OFFICIAL USE ONLY

- To specify that this is a mandatory profile, open the directory containing the profile and rename the file Ntuser.dat to Ntuser.man

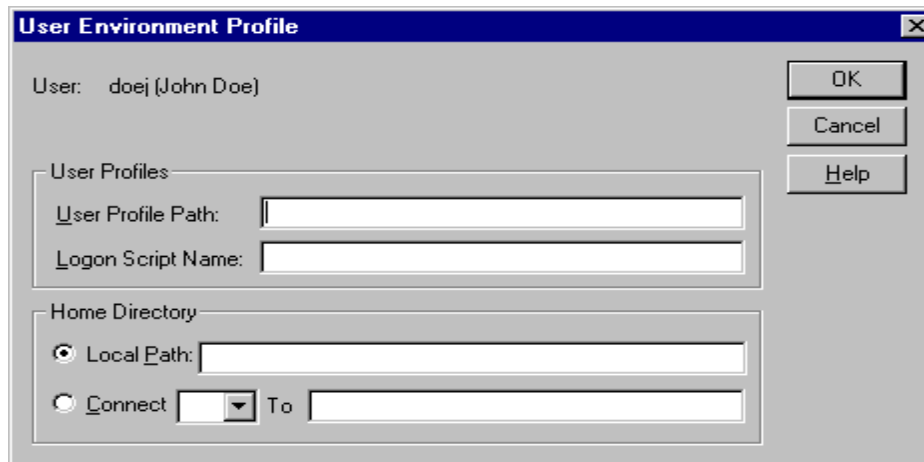


Figure 10 User Environment Profile

- Enter the **Logon Script Name** if it exists. Logon Scripts are executed during logon in environments where special procedures are required

NOTE: When using profiles, you must keep the following points in mind. A knowledgeable user can override profile settings so they must not be viewed as enforcing security.

Guidance on the use and configuration of user profiles can be found in the *Defense Information Infrastructure (DII) Common Operating Environment () Secure Windows NT Installation and Configuration Guide*.

6.1.10. Administrator Accounts

Because of the privileges associated with the Administrator account (by virtue of its membership in the Administrators group), access to this account must be strictly controlled. The following are some suggested guidelines for the Administrator account:

- Rename the administrator account (this can be done using the **Rename** option under the **User** menu in User Manager)

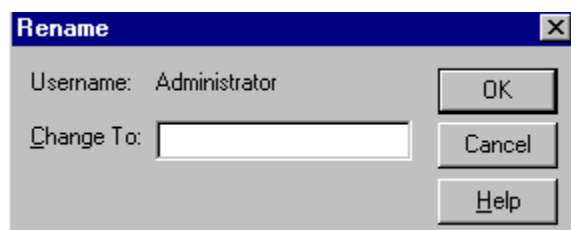


Figure 11 Renaming Users

FOR OFFICIAL USE ONLY

- Give administrators a separate personal account for their use when not performing tasks requiring the administrator account. Only log on using the administrator account when performing administrative functions. This is done via creation of new accounts that are represented in section 6.1.3
- Consider implementing an administrator password control process (such as writing down the password and storing it in a safe) to protect yourself from being unable to administer your system/domain due to a forgotten password
- Consider delegating administrative authority (i.e., separation of roles) by adding users to the Account Operators group
- If there are multiple administrators, create separate accounts for each so that their actions can be individually audited. This is done via creation of new accounts that are represented in section 6.1.3

Specific recommendations on securing administrative accounts can be found in the *Defense Information Infrastructure (DII) Common Operating Environment () Secure Windows NT Installation and Configuration Guide*.

6.2. System Policy

The System Policy Editor, available in Windows NT 4.0, can make granular restrictions to a User Profile, such as restricting any changes on the desktop or preventing access to the Control Panel or a command prompt. The use of the System Policy Editor is shown below.

- You can select users, groups, and computers to apply the policy to by selecting **Add User**, **Add Group**, or **Add Computer** from the **Edit** menu. This will result in additional icons displayed in the System Profile Editor window. Alternatively, you can edit the policy settings for the Default Computer and Default User icons so that one policy will apply to all computers and users within the domain

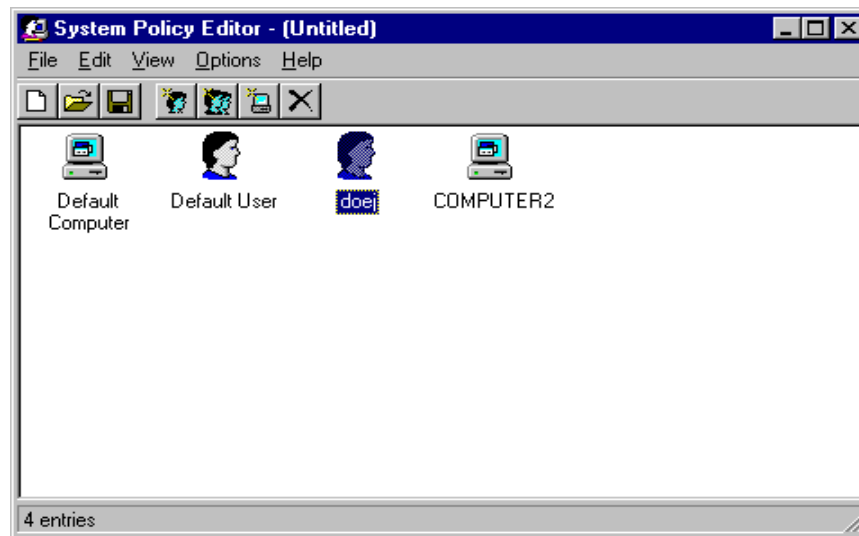


Figure 12 System Policy Editor

FOR OFFICIAL USE ONLY

- Double-clicking on an icon will bring up a Properties window that is used to specify the policy settings for that user or computer. (There is a different set of options available for computer policies and user policies.) The policy settings can differ across each user, group, or computer. The Properties dialog box shows six policies (Control Panel, Desktop, Shell, System, Windows NT Shell, Windows NT System) for users, and eight policies for computers (Network, System, Windows NT Network, Windows NT Printers, Windows NT Remote Access, Windows NT Shell, Windows NT System, Windows NT User Profiles) that can be edited to tailor a policy.
- Once editing is complete, the policy settings can be saved using the **Save** option on the **File** menu. This saves the policy settings in a file called NTCONFIG.POL
- Place the NTCONFIG.POL file in the Netlogon folder. Now when users log in using their domain accounts, the contents of the NTCONFIG.POL file are copied to the user's local computer Registry. The contents of the NTCONFIG.POL file are merged with the NTUSER.DAT profile file to create the user environment. Settings in the NTUSER.DAT file that conflict with settings in the NTCONFIG.POL file are overwritten; settings that do not conflict are retained

Specific recommendations on configuring system policies can be found in the *Defense Information Infrastructure (DII) Common Operating Environment Secure Windows NT Installation and Configuration Guide*.

6.3. User Rights Policy

User Rights can be granted to user accounts and groups to grant certain privileges to those accounts or groups. Each of these User Rights is described below, along with its default account assignments.

Table 6 User Rights

User Right	Description
Access computer from the network	Allows users to access NT resources over a network. By default this right is assigned to Everyone, Administrators, and Power Users groups.
Add workstations to the domain	Required at a domain level to add a new machine to that domain.
Log on locally	Allows users to log onto a Windows NT system interactively at the console. By default this right is granted to administrators and backup operators on workstations and servers. In addition it is granted to server operators, account operators, and print operators on servers and to power users, users, and guests on workstations.

FOR OFFICIAL USE ONLY

Bypass traverse checking	Permits a user to traverse subdirectories, even if that user has not rights to the parent directories. The default is this right is assigned to Everyone.
Back up files and directories	Permits the user to circumvent the file permissions for the purposes of backup and restore. By default this right is assigned to administrators, backup operators, and server operators.
Restore files and directories	A companion right to backup files and directories. By default this right is assigned to administrators and backup operators.
Change the system time	Allows the user to set the system time. By default this right is granted to administrators on workstations and servers and power users on workstations.
Create a page file	Permits users to create page files. By default this right is granted to administrators.
Create a token object	Allows the user to create security access tokens. By default no users are granted this right.
Create permanent shared objects	Allows users to create special permanent shared resources. By default this right is not granted to any user or group.
Debug Programs	Allows users to do low-level debugging. By default this right is granted to administrators.
Force shutdown from a remote system	Allows users to shut down a Windows NT system remotely. By default this right is granted to administrators on workstations and servers and to power users on workstations.
Increase Quotas	Allows users to increase object quotas. By default this right is granted only to administrators.
Increase scheduling priority	Allows users to increase the process priority of a given process. By default, this right is granted to administrators on servers and workstations, and power users on workstations.
Load and unload device drivers	Allows the user to load and unload device drivers from memory. By default, this right is granted only to administrators.
Lock pages in memory	Allows users to lock pages so they cannot be swapped out. By default no users are granted this right.
Log on as a batch job	Allows a user to log on using a batch queue facility (not currently supported). By default this right is granted only to administrators.

FOR OFFICIAL USE ONLY

Log on as a service	Allows a user to log on as a service. Services are background processes that run with direct user supervision; those that run under the system account have almost full control. By default no users are granted this right.
Manage Auditing and security log	Allows users to identify the types of user access that must be audited. In addition, this right grants the privilege of viewing and clearing the security log. By default, this right is granted to administrators.
Modify firmware environment	Allows the user to modify the system environment variables. By default this right is granted to administrators.
Profile single process	Allows users to use Windows NT performance monitoring tools to monitor the performance of a single process. By default this right is granted to administrators on workstations and servers, and power users on workstations.
Profile system performance	Allows users to monitor the performance of a Windows NT system using the monitoring tools. By default, this right is granted to administrators.
Replace a process-level token	Enables the user to replace the security access token. By default no users are granted this right.
Shut down the system	Permits the user to shut down the system from the system console. By default, this right is granted to administrators, backup operators, everyone, power users, and users.
Take ownership of files or other objects	Permits users to take control of any object in the system. By default, this right is granted only to administrators.
Act as part of the operating system	Permits the user to act as a trusted portion of the operating system and therefore be granted all rights to the system. By default no users are granted this right.

The following steps describe the procedure to change the assignment of any of these User Rights.

- Starting with the User Manager dialog box, Click **Rights** on the Policies menu to bring up the User Rights Policy dialog box.

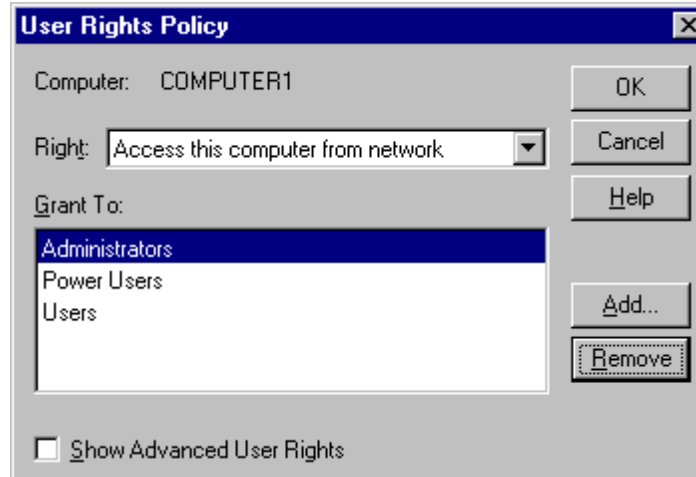


Figure 13 User Rights Policy Dialog Box

Note: Windows NT identifies some User Rights as standard and others as advanced.

- To show all the rights that can be assigned to a user or group, click on the combo box marked **Right**. Clicking on the box next to **Show Advanced User Rights** will show advanced user rights that can be assigned to a user or group
- To see what users or groups are assigned to a specific right, select a right using the process noted above. All of the users and groups who are assigned to that right will be shown in the box **Grant To**
- Rights can be assigned to groups or user accounts. To assign these rights, click the **Add** button and select the **group or user account** you wish to add. Click the **Ok** button when you have finished adding all groups or users
- A group or user account can also be removed from a right. To complete this task, select the desired **User Right** and then select the name of the user or group account in the **Grant To** box and click on the **Remove** button

6.3.1. Recommended Rights Assignments

User rights will be pre-assigned as the system is delivered from the factory and fielded to individual units. High-level recommendations for assigning User Rights can be found in the *NSA Guide to Securing Windows NT*.

6.4. Audit and Archive Log Policies

Windows NT provides three types of audit logs, which it refers to as Event Logs. They are the System Log, Security Log, and Application Log. The following discussion focuses on auditing security-relevant events and the use and configuration of the Security Log.

The SA will examine all event logs for misuse, system penetration or compromise, and to verify system security policy compliance. Audit trails must be reviewed for security

implications daily, but as a minimum will be reviewed once per week. The DAA will provide the policy for how long to maintain archived event logs.

6.4.1. Enabling Auditing

The first step in configuring auditing is to enable auditing and specify the types of events to be audited. To do this, perform the following steps.

- From the User Manager (or User Manager For Domains) administrative tool, select **Audit** from the Policies menu to bring up the Audit Policy dialog box

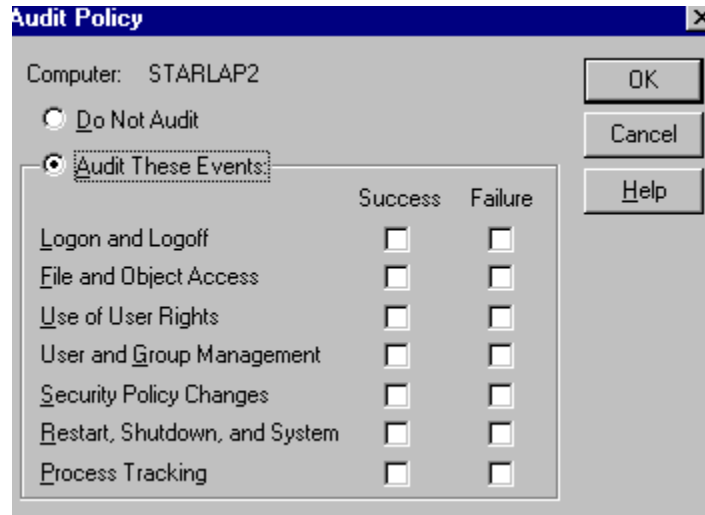


Figure 14 Audit Policy

- Select **Audit These Events** to enable auditing and check the desired events (see recommendations below). Options include the audit of **successful and/or failed**:
 - **Logon and Logoff** – records user’s local interactive logons and network logons. (*Success and Failure*)
 - **File and Object Access** – audits access to standard objects such as files, directories, and printers. (*Failure*)
 - **Use of User Rights** – records a users use of user rights. (*Access and Failure*)
 - **User and Group Management** – audits the creation, modification, and deletion of users and groups. This includes changing group membership, modifying account details, and updating user passwords. (*Success and Failure*)
 - **Security Policy Changes** – audits changes to audit policies, assignments of user rights, and establishment and removal of Windows NT Domain trust relationships. (*Success and Failure*)
 - **Restart, Shutdown, and System** – audits restarts and shutdowns of the system. (*Success and Failure*)

- **Process Tracking** – audits the indirect use of system rights. One example is a process acting on an object and a second is a process starting and stopping. (*Failure*)

6.4.2. Auditing Directories and Files

Once auditing of **File and Object Access** is enabled at the policy level, auditing must then be configured for the specific objects to be audited. To specify auditing on specific directories and files, perform the following steps:

- Select **Windows NT Explorer** from the **Program** Menu to bring up the Exploring dialog box
- Select the **desired directory or file** and click with the right mouse button
- Click on **Properties** to bring up the Properties dialog box shown in Figure 16
- Select the **Security** tab and click on the **Auditing** button to bring up the dialog box shown in Figure 16

Note: The File Auditing Dialog Box and Directory Auditing Dialog Box are the same except for Replace Auditing on Subdirectories or Replace Auditing on Existing Files options that are only given when auditing directories. Selecting Replace Auditing on Subdirectories will propagate the audit settings to all subdirectories within that directory. Specifying Replace Auditing on Existing Files will propagate the audit settings to each file in the specified directory.)



Figure 15 Auditing Directories & Files

FOR OFFICIAL USE ONLY

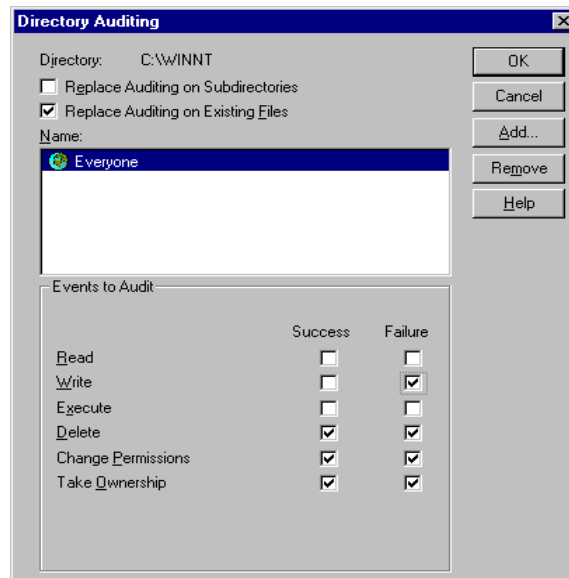


Figure 16 Auditing Users/Groups for Directories & Files

- Groups and users accounts can be added to the auditing process by clicking on the **Add** button shown in Figure 17
- Select the groups or user accounts to be added and then click the add button as shown in Figure 18. When all of the groups and users accounts have been added, select the **Ok** button to finish
- To remove groups or user accounts from the auditing process, select the **groups or user accounts** to be deleted and click the **Remove** button shown in Figure 17

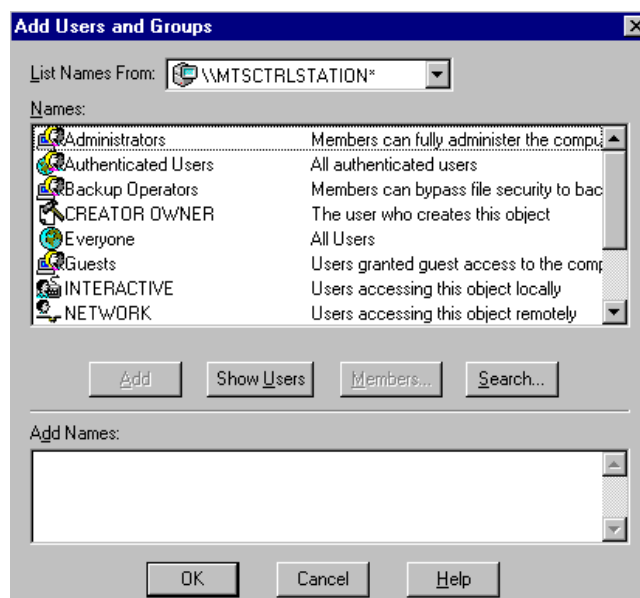


Figure 17 Adding Users/Groups for Auditing Directory & Files

FOR OFFICIAL USE ONLY

- For each specified user or group, select the events to be audited for the particular directory or file as shown in Figure 19. To accomplish this, highlight each **members name** and then select the appropriate events that will be audited (success and/or failure). Directory auditing options include auditing the success or failure of the following types of events:
 - **Read** - Audits the display of filenames, attributes, permissions, and ownership
 - **Write** - Audits the creation of subdirectories and files, changes to attributes, and display of permissions and ownership
 - **Execute** - Audits the display of attributes, permissions, and ownership as well as changing to subdirectories
 - **Delete** - Audits the deletion of the directory
 - **Change Permissions** - Audits changes to directory permissions
 - **Take Ownership** - Audits changes to directory ownership

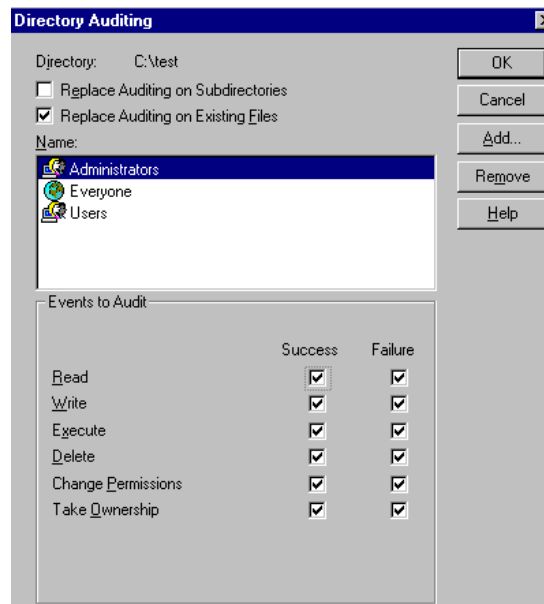


Figure 18 Auditing Users/Groups for Directories & Files

6.4.3. Auditing Printers

To enable the auditing of the use of printers, perform the following steps.

- From the **Start** Menu, select **Settings**, select **Printers**, right click on the target printer, click on **Properties**, click on the **Security** tab, and then the **Auditing** button to bring up the Printer Auditing dialog box

FOR OFFICIAL USE ONLY

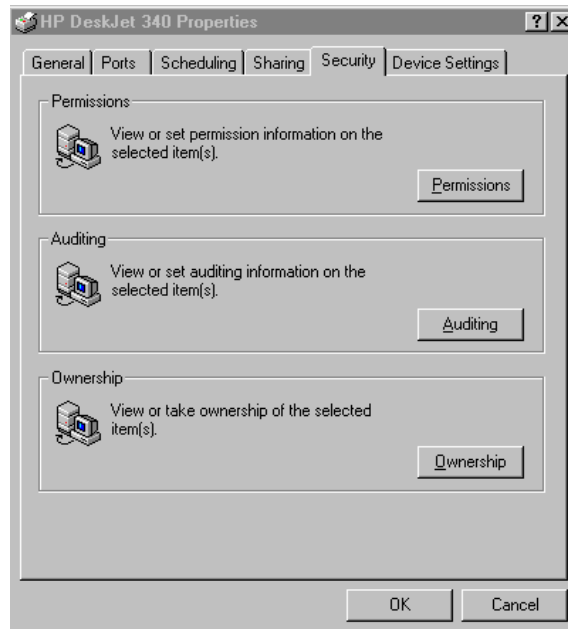


Figure 19 Auditing Dialog Box

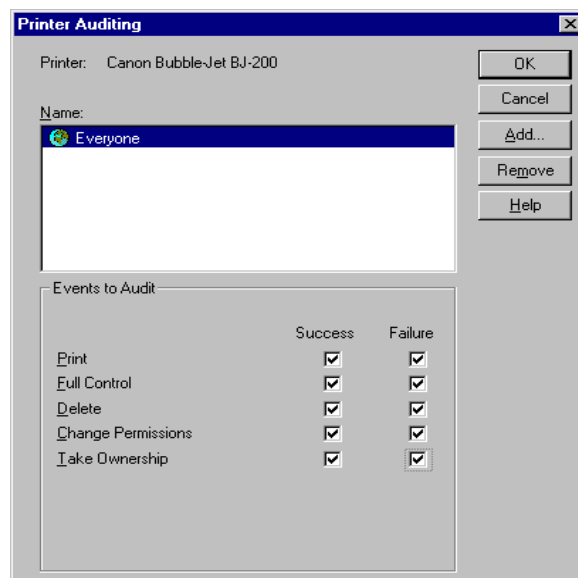


Figure 20 Auditing Users/Groups for Printers

- Use the **Add** or **Remove** button to add or remove groups or users to be audited from the **Name** box

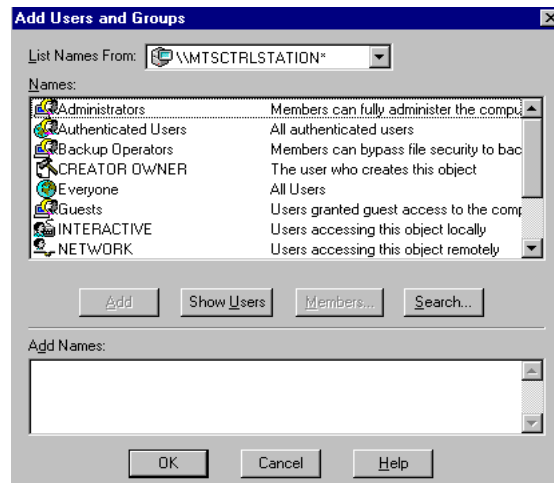


Figure 21 Adding Users/Groups for Auditing Printers

For each user or group, specify the events to audit. Full Control includes events that involve changing job settings, documents control, and sharing. The other events are self-explanatory. To audit events for a specific group or user, follow the steps below:

- To accomplish this, highlight each **members name**
- Select the appropriate events that will be audited (**success and/or failure**)

6.4.4. Auditing the Registry

Windows NT provides a capability to specify audit settings for each key in the registry. Procedures for configuring Registry auditing are as follows:

- Select **Run** from the **Start** menu and run **regedt32** (the Register Editor). Select the target key from the Registry Editor dialog box. Select the **Security** menu, then the **Auditing** option to bring up the following dialog box

NOTE: While working in the registry area, be extremely careful to not do anything outside of these instructions. Doing so could corrupt data on the MTS system.

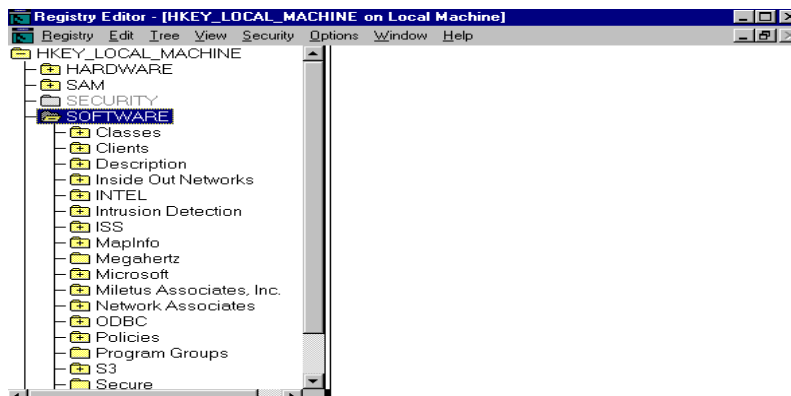


Figure 22 Auditing the Registry

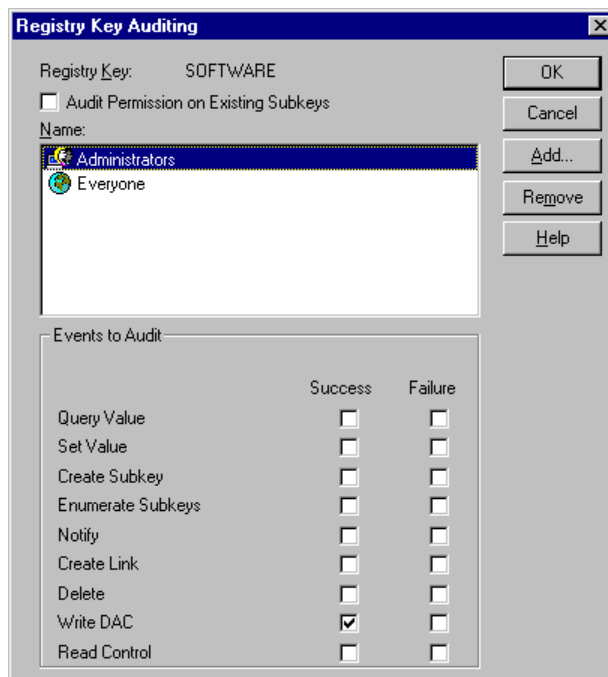


Figure 23 Auditing Users/Groups for the Registry

- Use the **Add** or **Remove** button to add or remove groups or users to be audited from the **Name** box

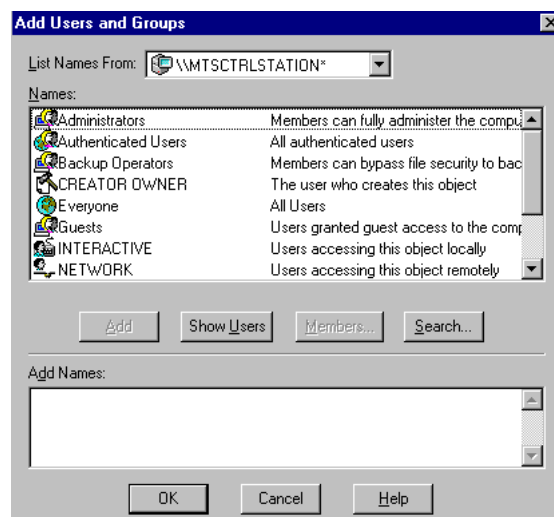


Figure 24 Adding Users/Groups for Auditing the Registry

Select each user/group and then select the events to be audited for that user/group.

- To accomplish this, highlight each members name and then select the appropriate events that will be audited (**success and/or failure**)

Specify the events to audit. Options include auditing the **success and/or failure** of each of the following types of events:

- **Query Value** – audits the success or failure of any request to read the value of the specified key.
- **Set Value** – audits the success or failure of a request to set the value of a key
- **Create Subkey** – audits the creation of new subkeys
- **Enumerate Subkeys** – audits user requests to list the subkeys of a given key
- **Notify** – audits a user request to open a key with Notify access
- **Create Link** – audits a user request to create a symbolic link to a registry key
- **Delete** – audits the deletion of registry key
- **Write DAC** – audits user requests to modify the permissions associated with a registry key
- **Read Control** – audits a user request to read the security data associated with a registry key
- Select **Audit Permission on Existing Subkeys** if you want to propagate the audit settings to all subkeys

6.4.5. Auditing Base Objects

Windows NT Base Objects are internal objects apart from the file system or the registry. In most cases, these system resources are not directly available to the user; rather, they are objects, which are accessible only through the Win32 API. These objects would normally not be audited, but if there is a need to audit them, it can be accomplished by following these steps:

- Set the system audit policy to audit object accesses

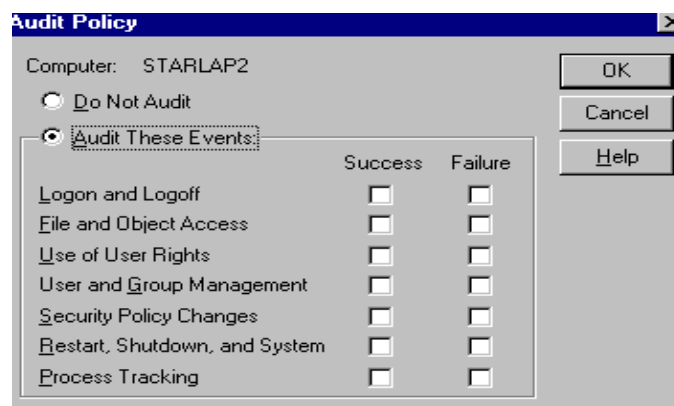


Figure 25 Audit Policy for Base Objects

FOR OFFICIAL USE ONLY

- Set the following registry key to a value of 1:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\AuditBaseObjects



Figure 26 Setting Registry Key Values

6.4.6. Auditing of Privileges

Certain privileges in the system are not audited by default even when auditing on privilege use is turned on. This is done to control the growth of audit logs. The privileges that are not audited include:

- Bypass traverse checking
- Debug programs
- Create a token object
- Replace process level token
- Generate Security Audits
- Backup files and directories
- Restore files and directories

To enable auditing of these privileges, do the following:

- Select the key: **\\HKEY_LOCAL_MACHINE\MTS Packet Switch\CurrentControlSet\Control\LSA**
- Ensure the “Full Privilege Auditing” key value exists and is set to 1

FOR OFFICIAL USE ONLY



Figure 27 Setting Registry Key Values

If the specified key value does not exist:

- Select “**Edit**” from the menu bar.
- Select “**Add Value**”.
- Enter “**FullPrivilegeAuditing**” in the “Value Name” box.
- Enter “**REG_BINARY**” in the data type box and then click the **OK** button

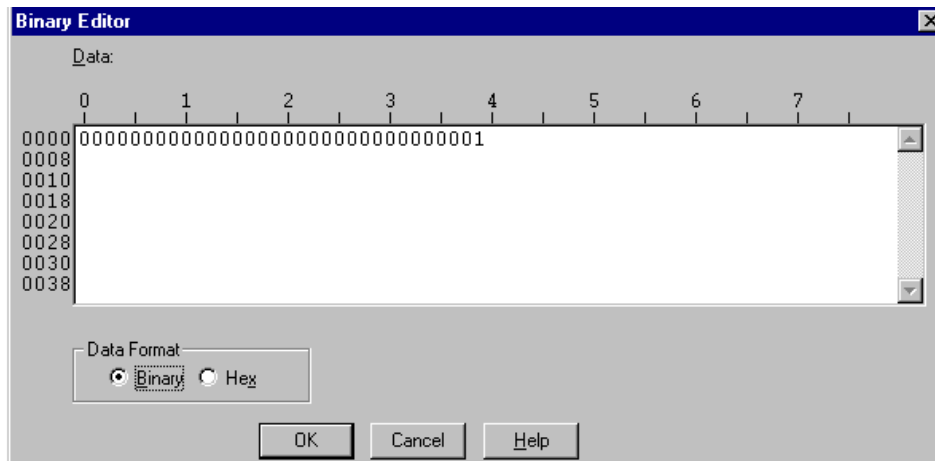


Figure 28 Binary Editor Box

- Enter “**00000001**” and select the **Binary** radio button in the “Binary Editor” box
- Click the **OK** button to finish

If the value exists, but is not set to 1:

- Select the incorrect value
- Select “**Edit**” from the menu bar

NOTE: See Figure 29 for the following instructions.

- Select **Binary**
- Enter “00000001” and select the **Binary** radio button in the “Binary Editor Box”
- Click the **OK** button to finish

6.4.7. Viewing Event Logs

Windows NT provides a tool to view the contents of the System, Security, and Application logs. This tool can be run by selecting the Start menu, Programs, Administrative Tools, then Event Viewer. This will open a window similar to that shown in Figure 30. The type of log to be viewed can be selected from the log menu.

The Event Viewer also allows filtering to help sort through the event logs. Filter options can be configured by selecting **Filter Events** from the Event Viewer’s View menu. The following filtering options are provided:

- **Dates** – filter events that occurred between the specified sets of dates and times
- **Types** – filter events based on their type, to include Information, Warning, Error, Success Audit, and Failure Audit
- **Source** – filter on the system process or resource (e.g., LSA, Security Account Manager, etc) that generated the logged event
- **Category** – filter on specified categories. The available categories depend on the selected source
- **User** – select the events in the log that were generated by a specific user
- **Computer** – filter the log and display the events associated with the activities of a specified computer
- **Event ID** – filter based on a specified event ID

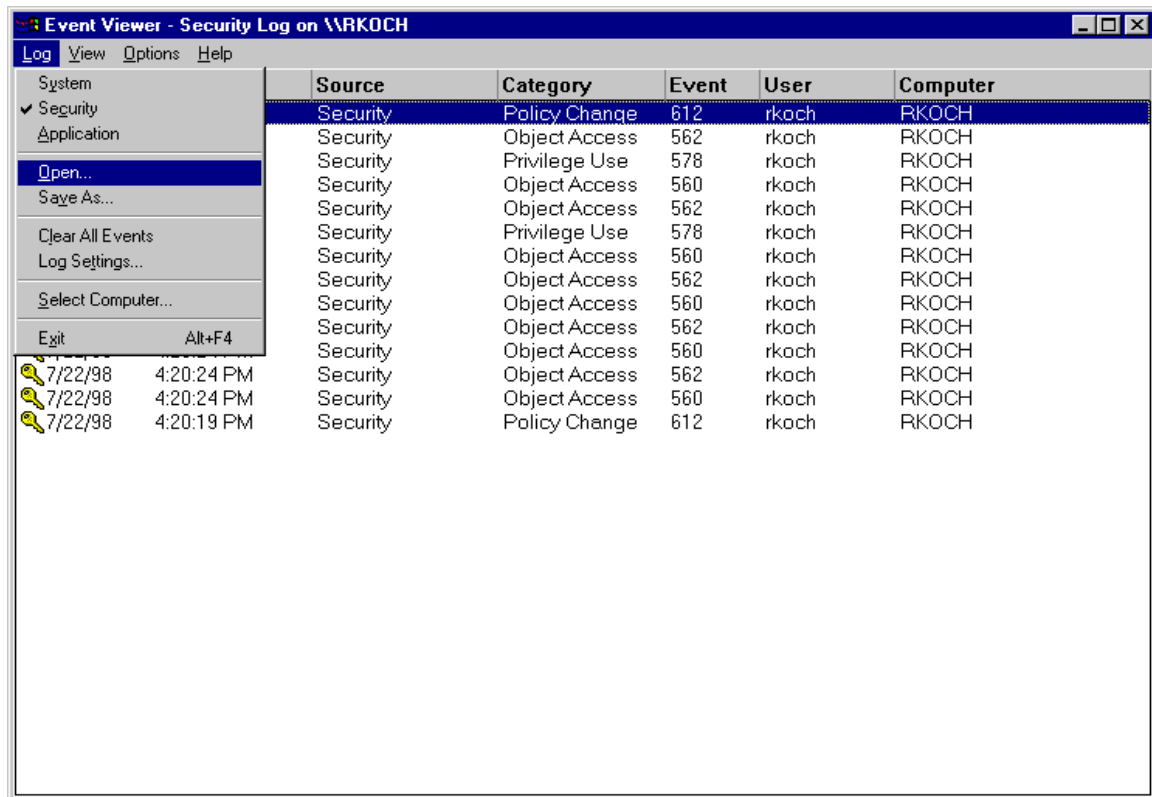


Figure 29 Viewing Event Logs

6.4.8. Setting Options for Log Events

For each log type, Windows NT allows the administrator to configure settings to control the size of the log and the actions to take when the log becomes full. Selecting **Log Settings** from the Event Viewer's Log menu configures the options shown in figure 31.

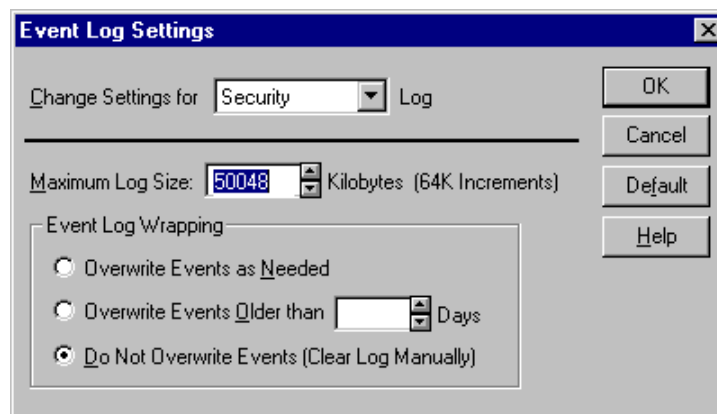


Figure 30 Options for Event Logs

FOR OFFICIAL USE ONLY

The Maximum Log Size is dependent on the sites audit policy and frequency of audit review, archival, and/or clearing. It is recommended that a minimum size of **2048 KB** be selected. This is noted in the U.S. Army memorandum called *Acert/CC Information Assurance/Vulnerability Alert (IAVA) Compliance Message 99-031, Securing Windows NT 4.0 Server/Workstation*.

Windows NT provides three options for reacting to a situation where the event logs become full. They are:

- **Overwrite Events as Needed** – this setting will allow audit events to be overwritten when the log becomes full, regardless of the age of the event
- **Overwrite Events Older than *n* days** - this setting will allow audit events that are older than the specified number of days to be overwritten when the log becomes full
- **Do Not Overwrite Events (Clear Log Manually)** – when the event log becomes full, no audit events will be written and an audit failure will result. The audit failure will result in one of two actions based on the value of the following registry key:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail

If this key has a value of 1, the system will perform an immediate shutdown when the log becomes full. If it has a value of 0, the system will continue to operate but audit data will be lost.

It is recommended that the **Do Not Overwrite Events** (Clear Log Manually) option be selected without the setting to shutdown the machine when the log becomes full. This requires a vigilant system administrator to regularly review and clear the logs before they become full.

6.4.9. Alternative Locations for the Security Log

By default, Windows NT keeps the active security log on the same logical drive as the WINNT directory. It is possible to change the location of the security log using the Registry Editor. This is accomplished by changing the “File” value of the following registry key:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Security

6.4.10. Archiving the Logs

Event Logs are broken down into three types; application, security, and system logs. The administrator on a regular basis to ensure there are no errors or security violations within MTS must examine these logs. These logs must also be regularly archived so as to ensure adequate space for the current logs to grow. The DAA for MTS will provide the policy for how long to maintain archived event logs. The following directions explain how to archive, verify archives, and recover archive logs within MTS.

- Click on the **Start Menu**
- **SELECT PROGRAMS**
- Select **Administrative Tools**
- Select **Event Viewer**

6.4.11. Archiving Event Logs

Select the type of log you wish to archive:

- Application Log
- Security Log
- System Log

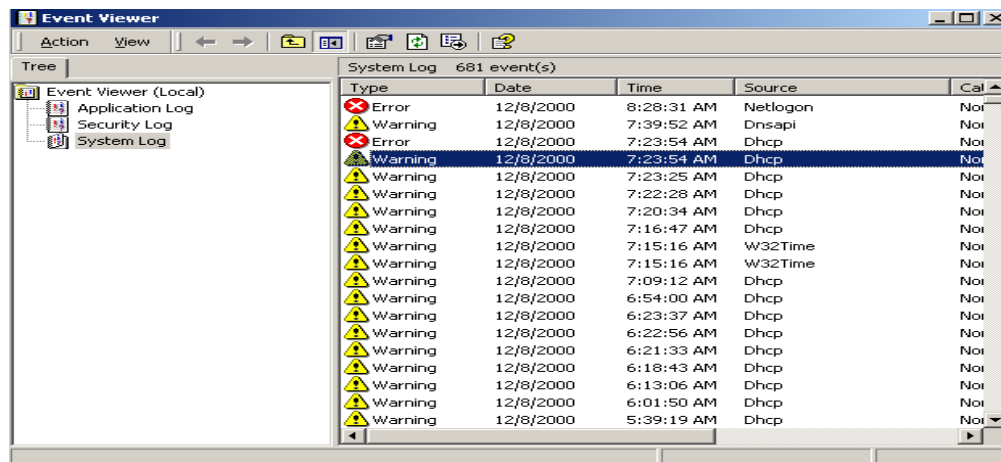


Figure 31 Archiving Event Logs

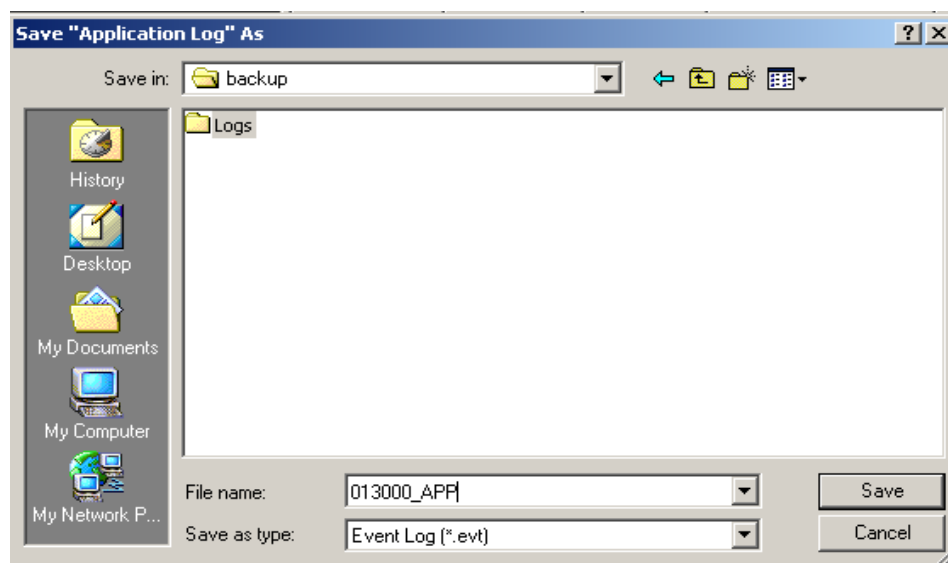


Figure 32 Save As Option for Event Logs

- Right-click on the selected log type and select **Save Log File As**
- Select the drop down box located at the top of the new window
- Select **D:\Logs**
- Edit the **file name** to follow one of the formats noted below:

NOTE: The file name must consist of the following format (*MMDDYY_Type of Log*). Where *MM* = the two digit month, *DD* = the two digit day, and *YY* = the two digit year. *Type of Log* = *APP* for Application Log, *SEC* for Security Log, and *SYS* for System Log.

Examples: 013000_APP
113000_SYS

- Click on the **SAVE** button

6.4.12. Verifying Saved Event Logs

To verify saved event logs:

- Click on **My Computer** to located files or directories
- Verify that the file was saved in **D:\Logs**

6.4.13. Clearing Event Logs

When clearing event logs, use the steps below

- Click on the type of log you wish to clear:
 - Application Log
 - Security Log
 - System Log
- Right-click and select **Clear All Logs**

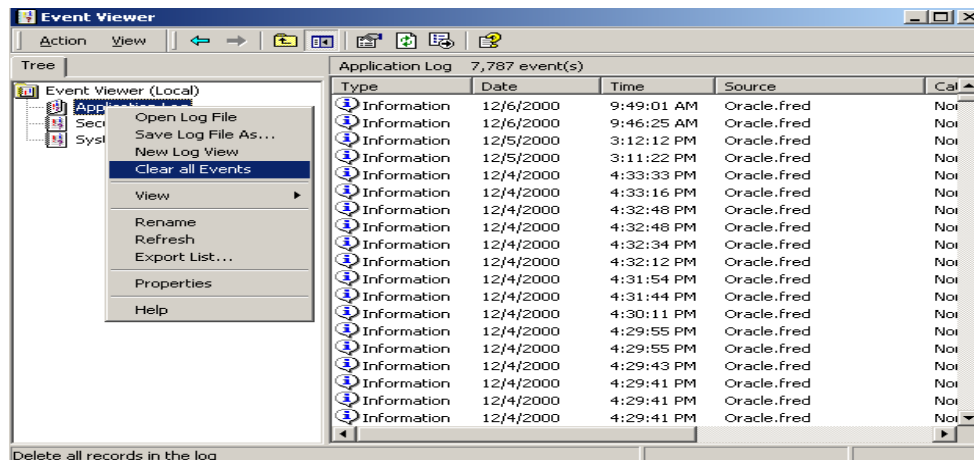


Figure 33 Clearing Event Logs - #1

- Select the **NO** button

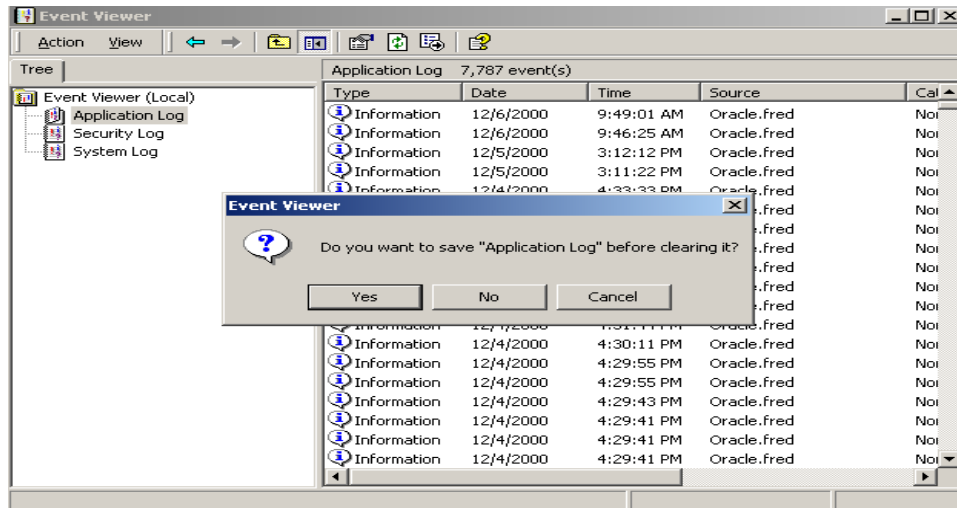


Figure 34 Clearing Event Logs - #2

6.4.14. Restoring Event Logs

- Click on the type of log you wish to restore:
 - Application Log
 - Security Log
 - System Log
- Right-click and select **Open Log File**

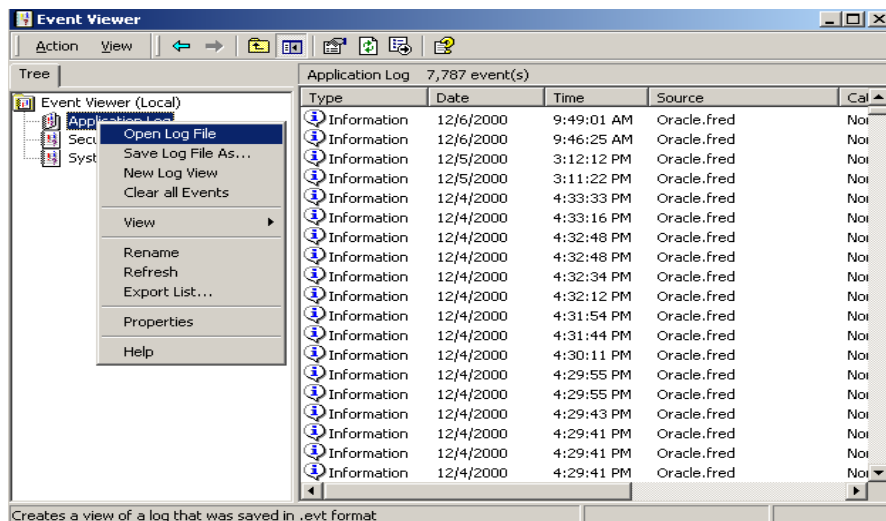


Figure 35 Restoring Event Logs

- Locate the log file you wish to restore in **D:\Logs**

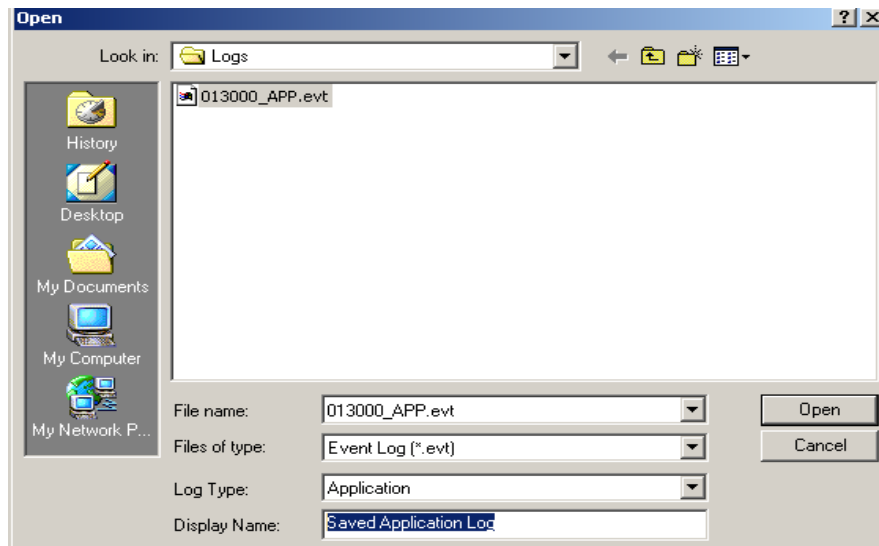


Figure 36 Locating Archived Event Logs

- Select the Log Type (**Application, Security, or System**) you are restoring
- Edit **Display Name** or leave it as the default
- Click on the **OK** button

6.4.15. Recommendations for Auditing

High-level recommendations for configuring the audit policy can be found in the *Defense Information Infrastructure (DII) Common Operating Environment () Secure Windows NT Installation and Configuration Guide*.

6.5. Managing Printers

Under Windows NT, support access to printers is controlled through ACL settings. Selecting the **Security** tab in the printer properties dialog box shown in Figure 20 and then selecting the **Permissions** button allows the configuration of printer ACLs. The permissions that can be specified to control access to the printer are:

- **Full Control** – Allows all rights over a printer, including printing, starting and stopping print queues, changing a print job order, changing printer properties, deleting printers, and changing printer permissions. By default, this is granted to Administrators, Print Operators, and Server Operators
- **Print** – Allows users to print documents on the given printer. By default, the “Everyone” group is granted Print access to all new printer shares
- **Manage** – Allows users to control document settings and start, stop, or pause specific print jobs. By default, this is granted to the creator or owner of the document submitted for printing

- **No Access** – Denies access to a printer

The use of printers can also be audited, as was discussed in section 6.4.3.

In addition, under Windows NT print jobs are spooled to disk before printing. By default, print jobs are spooled to the Winnt\System32\spool directory. Users who need to create print spool files must have permission to create new files in the spool directory. (The default permissions on this directory include providing Read access to the Everyone group and Full Control to the Creator Owner group.)

6.6. Setting Registry Size Limit

The Windows registry is one of the most vital parts of a computer system. The U.S. Army sent out a memorandum called *Acert/CC Information Assurance/Vulnerability Alert (IAVA) Compliance Message 99-031, Securing Windows NT 4.0 Server/Workstation*. This memo discusses the maximum size for the Windows registry and the process for setting it within Windows NT. This process is noted below:

- Select **Start**, select **Settings**, select **Control Panel**, and select the **System icon**
- Select the **Performance tab**
- Click on the **Change** button

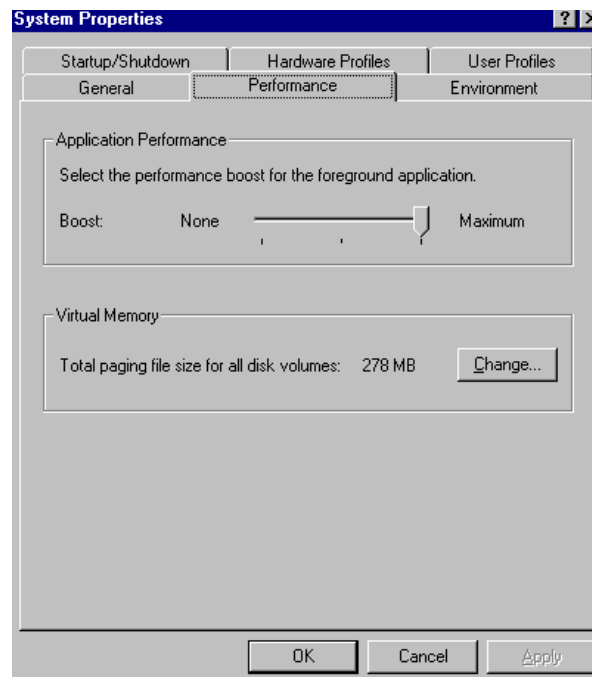


Figure 37 System Properties

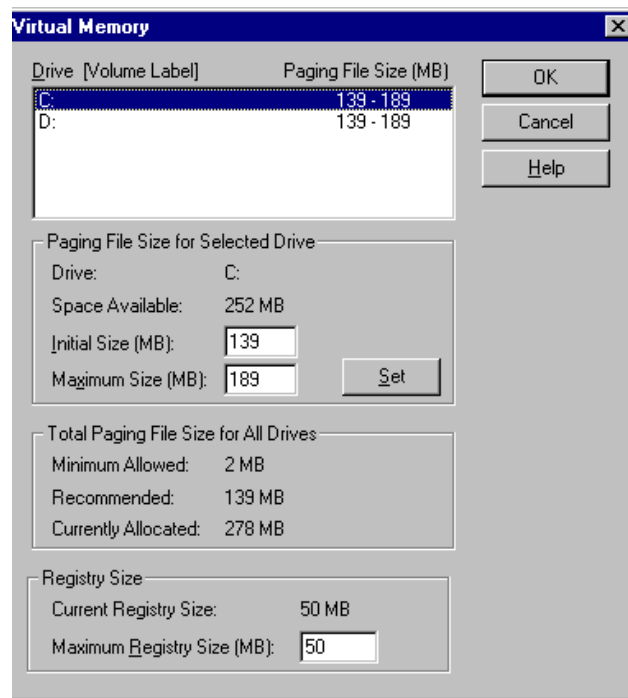


Figure 38 Registry Size Settings

- Select either the **C:** or **D:** drive noted in Figure 39
- Enter **40** into the box marked **Maximum Registry Size {MB}**
- Select the other drive **C:** or **D:** that was not selected in previously
- Enter **40** into the box marked **Maximum Registry Size {MB}**
- Click on the **OK** button
- Click on the **OK** button
- Close the open Control Panel window

6.7. Performance Monitor

The Performance Monitor is an administrative tool provided with NT for monitoring system performance. Performance Monitor can also help spot the activity of a virus (by spotting performance degradation) or an attempted break-in (by tracking logon attempts). The Performance Monitor can be set to send an alert to one or more administrators when certain events occur.

Figure 39 shows the Performance Monitor tool for Windows NT. The Performance Monitor is available under the Administrative Tools (Common) menu list. When the Performance Monitor is started the graph is empty. To begin monitoring system resources, choose the Edit, Add to Chart menu item which opens the Add to Chart dialog box.

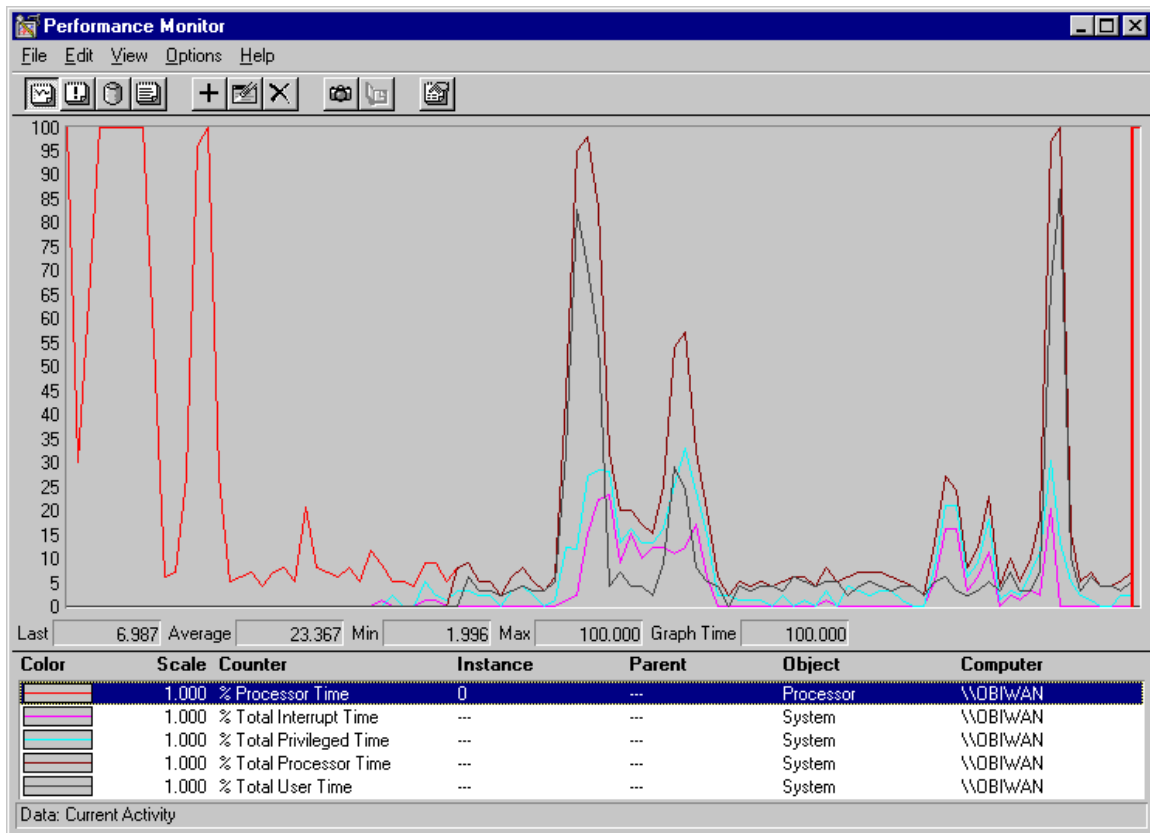


Figure 39 Performance Monitor

Within the Add to Chart dialog you can specify the computer you want to monitor, the object you want to monitor, and the particular counter from that object. In Windows NT all resources are described as objects. For example, Figure 40 shows the Processor object and several of the Counters you can monitor about it.

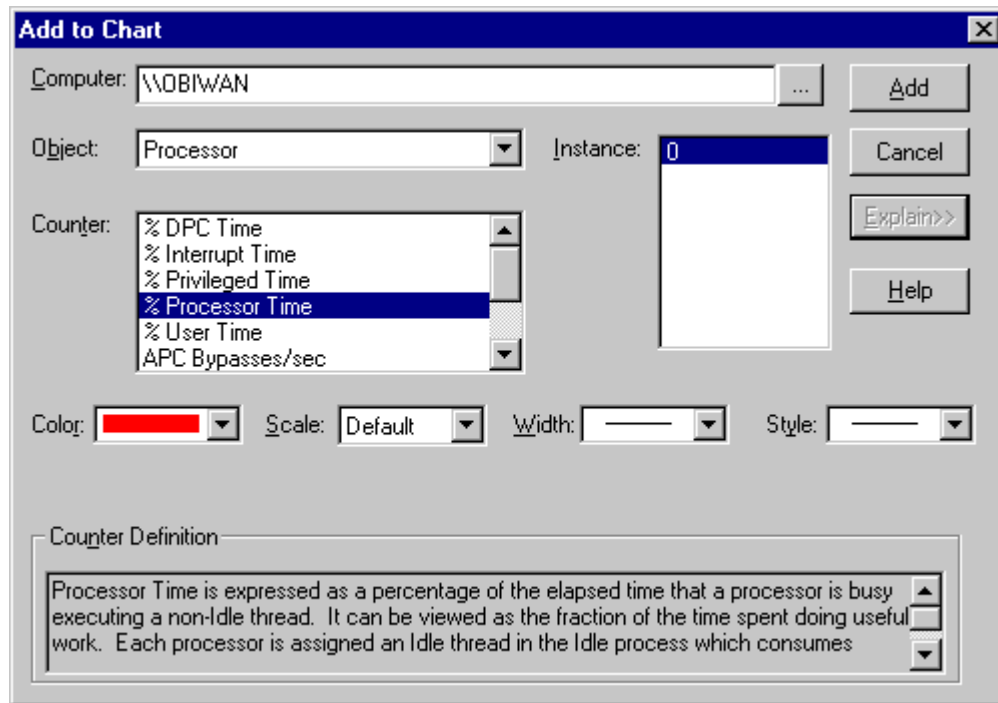


Figure 40 Selecting Counters to Chart

The Performance Monitor program can also be used to alert administrators when thresholds have been crossed for monitored items. This is useful if you are monitoring disk capacity, network errors, disk errors, etc. Setting up alerts is the same as Chart monitoring except in addition to this, you set up a threshold value and an optional program to run when the threshold is exceeded. Figure 41 shows the Alert monitoring screen.

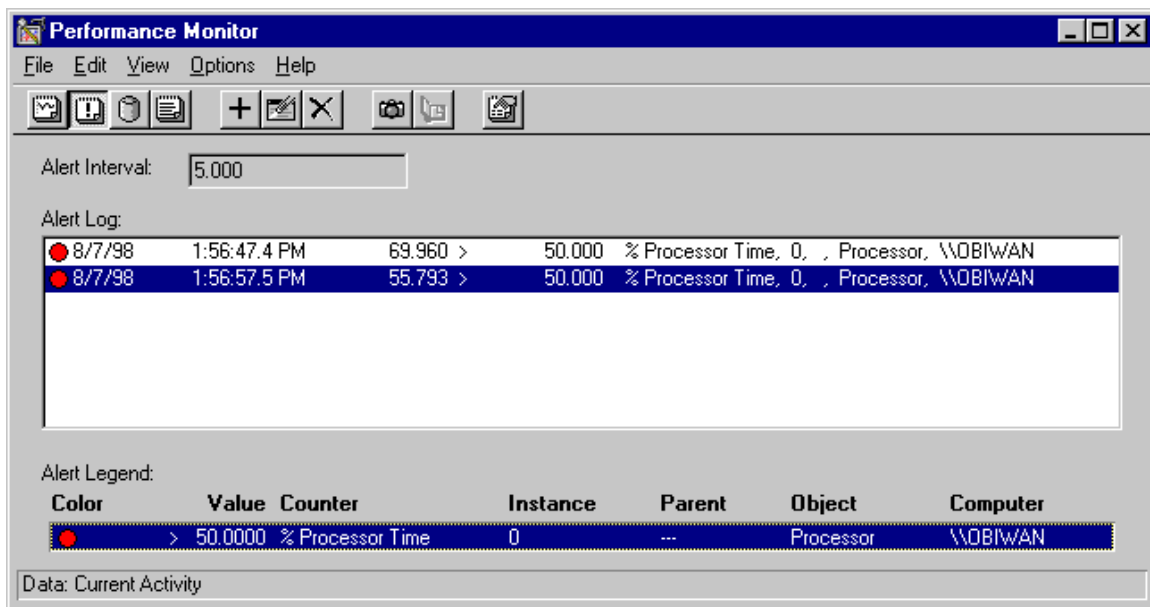


Figure 41 Alert Monitoring

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

7. ACCESS CONTROLS

This section presents procedures and recommendations for setting access controls on the file system and the Registry. Access controls will be pre-assigned as the system is delivered from the factory and fielded to individual units. These configurations will be IAW with DoD and Army Regulation.

7.1. File System Access Controls

Windows NT 4.0 supports two file systems: the FAT file system (as is used in DOS and Windows 95/3.1) and the NTFS file system. Only the NTFS file system provides access control capabilities. These access control capabilities are implemented using Access Control Lists (ACLs). An ACL is associated with an object (e.g., files and directories) and specifies the users or groups that can access that object and what permissions they have to the object.

Each object (defined as a discretely named resource within the system) has a pair of access control lists associated with it: a Discretionary ACL (DACL) and a System ACL (SACL). The DACL represents permissions, which may be assigned, to users while the SACL is set by the system security policies (for example, a files SACL may specify to audit all file reads).

7.1.1. File Permissions

At the Windows NT explorer interface, the following permissions can be granted on files:

- **No Access (None)** – Prevents any access to the file. Specifying No Access for a user prevents that user from accessing the file even if the user is a member of a group that has access to the file
- **Read (RX)** – Allows viewing of the file's data and running the file if it is a program
- **Change (RWXD)** – Allows viewing the file's data, running the file if it is a program file, changing data in the file, and deleting the file
- **Full Control (All)** – Allows viewing the file's data, running the file if it is a program file, changing data in the file, deleting the file, changing permissions on the file, and taking ownership of the file
- **Special Access** – Allows specifying the access at a lower level of granularity

Special Access options include:

- **Read (R)** - Allows viewing the file's data
- **Write (W)** - Allows changing the file's data
- **Execute (X)** - Allows running the file if it is a program file
- **Delete (D)** - Allows deleting the file
- **Change Permissions (P)** - Allows changing the file's permissions

- **Take Ownership (O)** - Allows taking ownership of the file

To set the permissions on files, use the following procedure:

- From the **Start** button, select **Program**, choose **Windows NT Explorer**
- Locate the target file and click on its name with the right mouse button
- On the menu that appears, select **Properties**
- In the subsequent window, click on the **Security** tab and then click on **Permissions** to bring up the Permissions dialog box

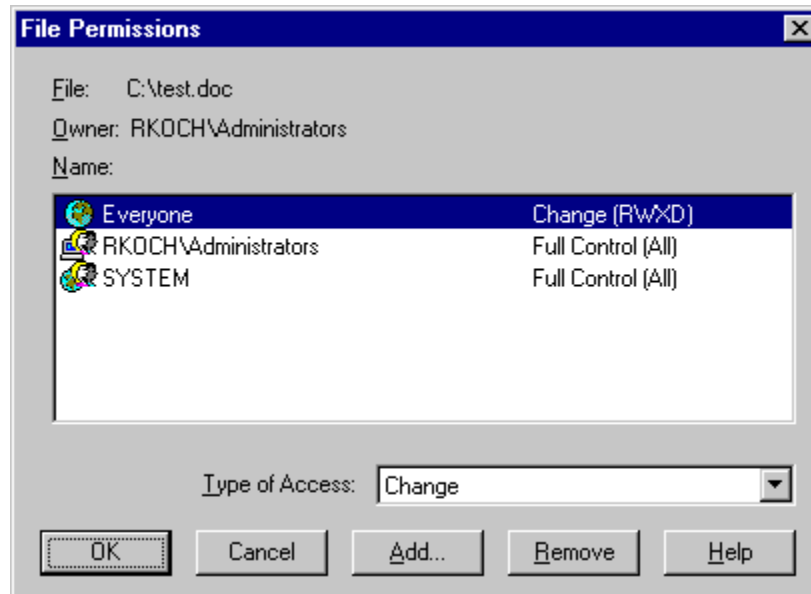


Figure 42 File Permission Dialog Box

- Use the **Add** or **Remove** buttons to add/remove users and/or groups to/from the access list
- Use the Type of Access pull-down menu to select the desired type of access for each group/user on the access list

7.1.2. Directory Access Permissions

When you set permissions on a directory, two sets of abbreviations for individual permissions are displayed. The first is the permissions set on the directory itself and the second are the permissions set on files in the directory.

For example, if you set Add & Read permission on a directory, you see (RWX), signifying Read, Write, and Execute permissions on the directory, and (RX) signifying Read and Execute permission on files in the directory. When access to files is shown as (Not Specified), that group or user cannot use files in the directory unless access is granted by another means; for example, by setting permissions that grant access on the individual files. An asterisk (*) following the set of directory permissions, for example

FOR OFFICIAL USE ONLY

(All)*, indicates that subdirectories do not inherit the permissions granted to that group or user.

Setting permissions on a directory specifies the access that a group or user has to the directory and, by default, its files. Existing subdirectories and their files are not changed unless you specify to change them. However, when you create new files and subdirectories in the directory, they inherit their permissions from the directory.

Permissions are cumulative. For example, if a user is a member of a group with Read permission and a member of a group with Change permission, the user will have Change permission. The one exception is that the No Access permission overrides all other permissions.

At the Windows NT explorer interface, the following permissions can be granted on directories:

- **No Access (None)(None)** - Prevents any access to the directory and its files. Specifying No Access for a user prevents access even if that user belongs to a group that has access to the directory
- **List (RX)(Not Specified)** – Allows viewing filenames and subdirectory names and changing to the directory's subdirectories. Does not allow access to files, unless granted by other directory or file permissions
- **Read (RX)(RX)** – Allows viewing filenames and subdirectory names, changing to the directory's subdirectories, and viewing data in files and running applications
- **Add (WX)(Not Specified)** – Allows adding files and subdirectories to the directory. Does not allow access to files, unless granted by other directory or file permissions
- **Add & Read (RWX)(RX)** – Allows viewing filenames and subdirectory names, changing to the directory's subdirectories, viewing data in files and running application files, and adding files and subdirectories to the directory
- **Change (RWXD)(RWXD)** – Allows viewing filenames and subdirectory names, changing to the directory's subdirectories, viewing data in files and running application files, adding files and subdirectories to the directory, changing data in files, and deleting the directory and its files
- **Full Control (All)(All)** – Allows viewing filenames and subdirectory names, changing to the directory's subdirectories, viewing data in files and running application files, adding files and subdirectories to the directory, changing data in files, deleting the directory and its files, changing permissions on the directory and its files, and taking ownership of the directory and its files. It must also be noted that groups or users granted Full Control permission on a directory can delete files in that directory no matter what permissions are on the files
- **Special Directory Access** – Allows the specification of more granular permissions on the directory. Options include:

FOR OFFICIAL USE ONLY

- **Read (R)** - Allows viewing the names of files and subdirectories
- **Write (W)** - Allows adding files and subdirectories
- **Execute (X)** - Allows changing to subdirectories in the directory
- **Delete (D)** - Allows deleting the directory
- **Change Permissions (P)** - Allows changing the directory's permissions
- **Take Ownership (O)** - Allows taking ownership of the directory
- **Special File Access** – Allows the specification of more granular permissions on the files within the directory. Options include:
 - **Read (R)** - Allows viewing the file's data
 - **Write (W)** - Allows changing the file's data
 - **Execute (X)** - Allows running the file if it is a program file
 - **Delete (D)** - Allows deleting the file
 - **Change Permissions (P)** - Allows changing the file's permissions
 - **Take Ownership (O)** - Allows taking ownership of the file

To set the permissions on directories, use the following procedure:

- From the Start, Program menu choose Windows NT Explorer
- Locate the target directory and click on its name with the right mouse button
- On the menu that appears, select Properties
- In the subsequent window, click on the Security tab and then click on Permissions to bring up the Permissions dialog box

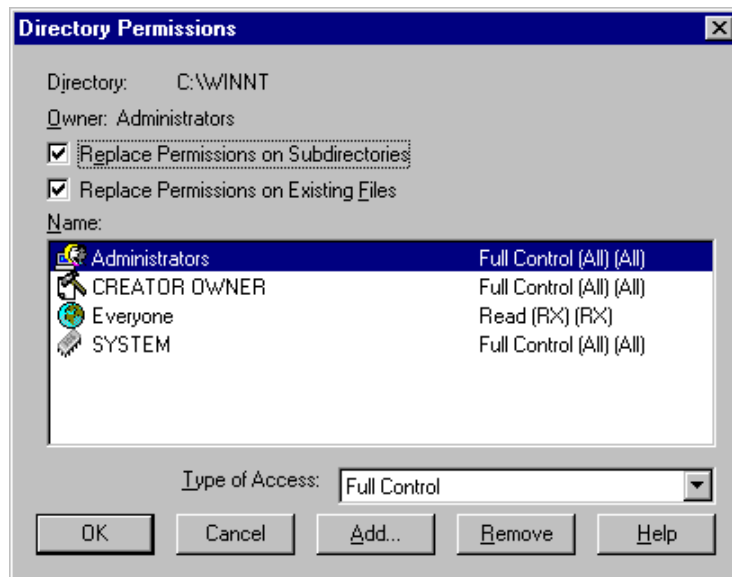


Figure 43 Directory Permissions for Users/Groups

- Use the **Add** or **Remove** buttons to add/remove users and/or groups to/from the access list
- Use the Type of Access pull-down menu to select the desired type of access for each group/user on the access list

Determine whether you want to apply the permissions only to the directory; to the directory and the existing files (this is the default); or to the directory, existing files, subdirectories, and their files. This is controlled by the “Replace Permissions on Subdirectories” and Replace Permissions on Existing Files” options.

7.1.3. File and Directory Ownership

Files and directories are initially owned by their creator. The owner of a file or directory has the ability to specify permissions on that object. By default, Administrators have the ability to take ownership of any file or directory on a system. An object owner can also grant permission to take ownership of an object to another user or group. Anyone with permission to take ownership of an object can exercise that right and then assign new permissions for that object. To take ownership of an object, perform the following steps:

- From the **Start** menu, select **Program**, choose **Windows NT Explorer**
- Locate the target file and click on its name with the right mouse button.
- On the menu that appears, select **Properties**.
- In the subsequent window, click on the **Security** tab and then click on **Ownership** to bring up the Owner window
- Click on the **Take Ownership** button.

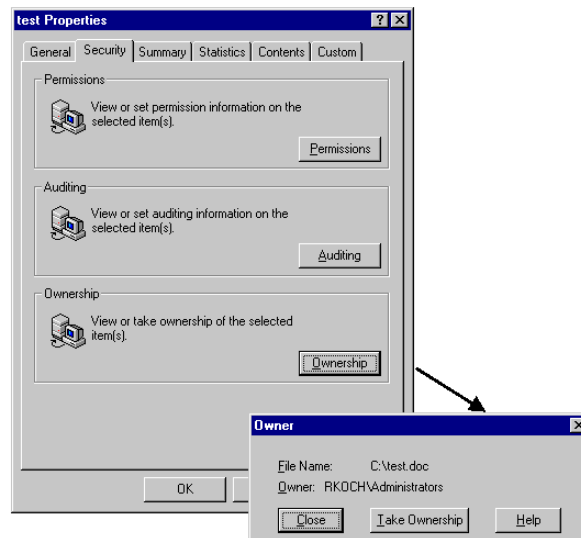


Figure 44 Taking Ownership of Files

7.2. Registry Access Controls

The initialization and configuration information used by Windows NT is stored in the Registry. Hence, it is important to protect the contents of the Registry from unauthorized modifications.

Similar to files and directories, access to Registry keys is protected through the use of ACLs. The basic permissions that can be granted on a key value are:

- **Q** = query value (read a key's values)
- **S** = set value (write a key's values)
- **C** = create a subkey
- **E** = enumerate subkeys (read names of subkeys)
- **N** = receive notification when key changes
- **D** = delete the key
- **R** = read key's ACL

For convenience when specifying permissions on Registry keys, some of these basic permissions were grouped into higher-level "permissions", including:

- **Read** = QENR
- **Add** = QCENR
- **Full Control** = QSCENDR

To specify permissions on Registry keys, perform the following steps:

- From the **Start** menu, click on **Run**, type **Regedt32** and click on the **Ok** button. This will open the Registry Editor.

NOTE: Registry Editor must be used only by individuals who thoroughly understand the tool, the registry itself, and the effects of changes to various keys in the registry. Mistakes made in Registry Editor could render part or all of the system unusable.

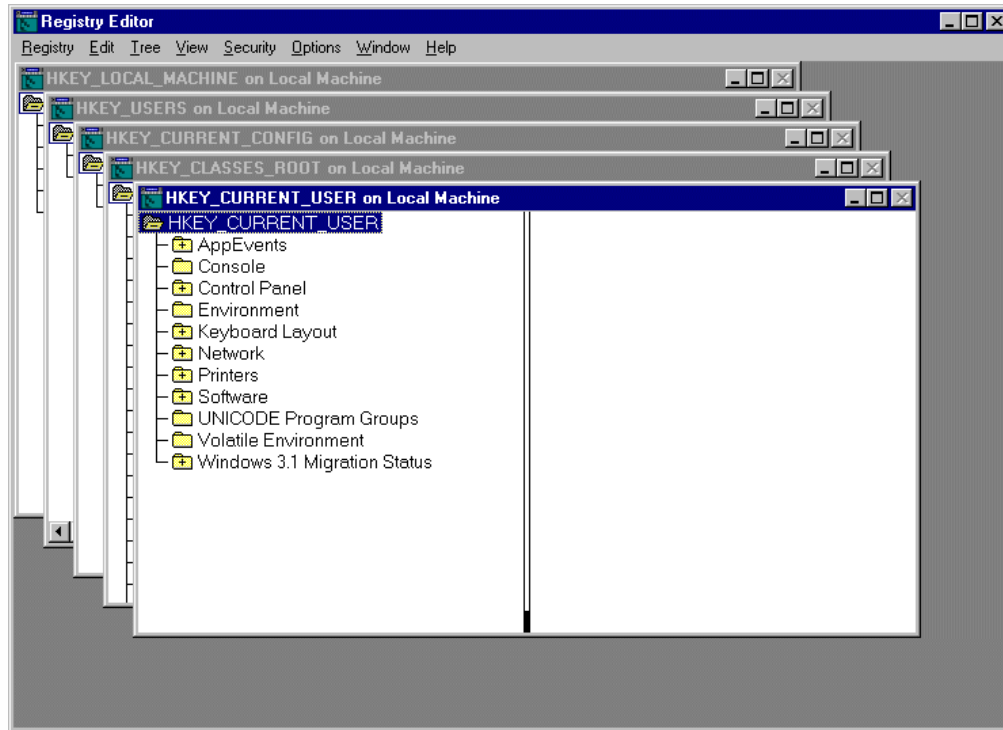


Figure 45 Registry Editor

- Click on the target Registry key, Click on the **Security** menu, then click on **Permissions** to bring up the Registry Key Permissions dialog box shown in
- Use the **Add** and **Remove** buttons to create the list of accounts to grant access to
- Use the **Type of Access** button to specify the type of access to grant to each account
- Determine whether to propagate the permissions to any existing subkeys
- Click on **OK**.

The Registry Editor can also be used to add new Registry keys and add/edit key values (from the **Edit** menu). Recommendations for adding and/or editing certain Registry keys to improve the security of systems can be found in the *Defense Information Infrastructure (DII) Common Operating Environment () Secure Windows NT Installation and Configuration Guide*.

Use of **Regedt32** to secure the Windows NT registry is noted in the U.S. Army memorandum *Acert/CC Information Assurance/Vulnerability Alert (IAVA) Compliance Message 99-031, Securing Windows NT 4.0 Server/Workstation*. This memorandum is located at the following web address:

<https://akocomm.us.army.mil/c2p/nsip/iapol/messages/042100zmar99.htm>

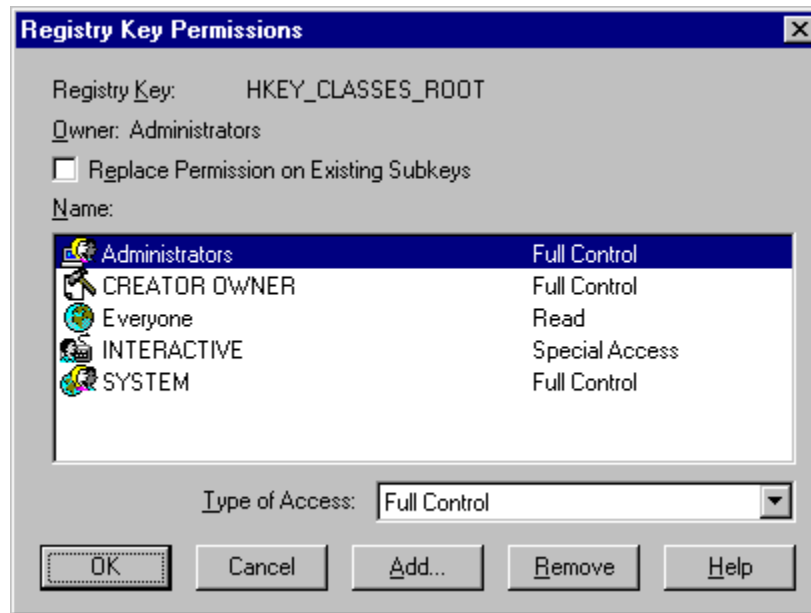


Figure 46 Registry Permissions

7.3. Recommended Permissions for Files, Directories, and Registry Keys

Specific recommendations for specifying permissions on files, directories, and Registry keys can be found in the *Defense Information Infrastructure (DII) Common Operating Environment () Secure Windows NT Installation and Configuration Guide*.

7.4. Locking the Workstation

When leaving the workstation for any length of time, users must either log off or lock the workstation in order to protect the workstation and the user's data from passers-by who can take advantage of the open session. MTS security policy requires users to utilize the terminal lock feature to prevent unauthorized access to the system and sensitive data. Prior to leaving a terminal unattended, the user must activate the terminal lock feature. Once executed, the monitor will display a blank screen and prevent anyone from viewing sensitive data. After the terminal lock feature is activated, future access to the terminal is granted only after entry of a valid User ID and password.

7.4.1. Automatic Locking

The user can configure the workstation to automatically lock itself after a set period of time by selecting a screen saver that has the Password Protect option. This feature should only be activated when it does not hinder the users ability to access the system. To configure the Workstation to lock itself with a screensaver after a specified period of inactivity, perform the following steps:

- Double-click on "My Computer"

FOR OFFICIAL USE ONLY

- Double-click on “Control Panel” and then double-click on the “Display” icon to bring up the window shown in the figure below

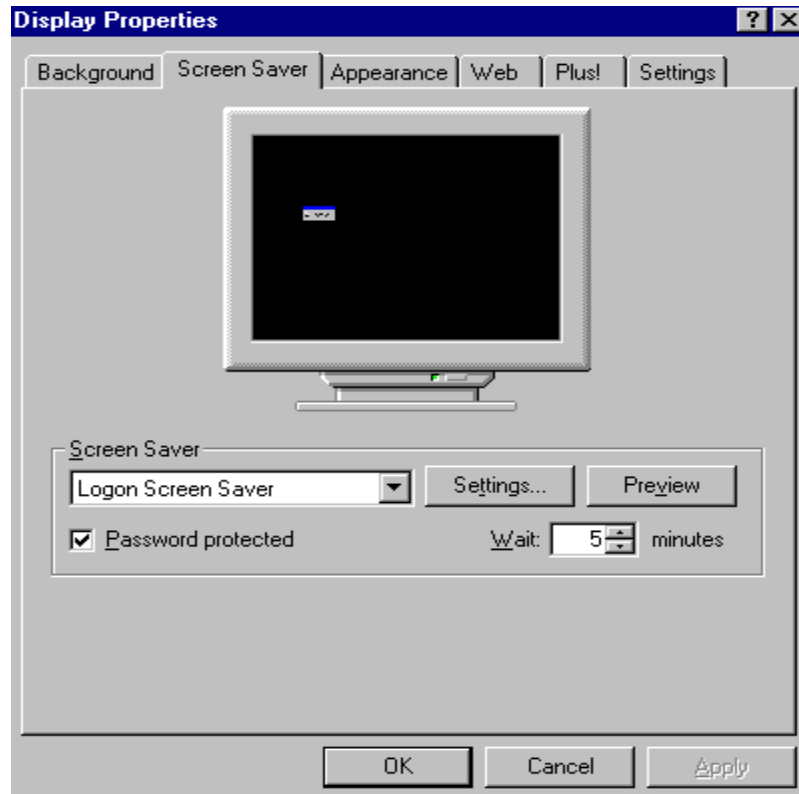


Figure 47 Screensaver Settings

- Click on the Screen Saver tab
- Select the 32-bit screen saver that displays a “Logon Screen Saver”
- Click the “Password protected” checkbox to enable the lock out feature and then set the amount of time before it is invoked. The amount of time must be set at 3 to 5 minutes. This is in accordance with AR 380-19 paragraph 2-11c(3 and 2-11c(4

Note: The password that will be used when this screen saver is invoked is the one that was given to the user when his/her MTS account was created on this workstation.

- Click on OK

7.4.2. Manual Locking

- To manually lock your workstation, press **CTRL+ALT+DEL** and then choose the “**Lock Workstation**” button in the Windows NT Security dialog box.

FOR OFFICIAL USE ONLY

- To unlock your workstation, press **CTRL+ALT+DEL** and type your password into the “**Workstation Locked**” dialog box

7.4.3. Logging off the System

Logging off a MTS workstation allows other users with valid accounts to use the machine without disrupting the previous user’s data, whereas locking the workstation locks the interactive user interface but does not close the currently active processes of the user logged in to the workstation. Logging off the system at the end of the workday or before a long absence is mandatory.

To logoff of the MTS follow the steps below:

- Click on the **Start** button
- Click **Shutdown**
- Click the **OK** button

8. SYSTEM INSTALLATION FOR MTS SOFTWARE

MTS specific software is installed and configured by COMTEC on the Control Station and V2's. While the V2 or Control Station is in use, the system at some point might experience some software problems that will need to be addressed by the MTS SA. If the SA determines that he or she cannot fix the software problem then the system will be returned to COMTEC where it will be re-outfitted with the current MTS software.

9. UNIX SECURITY ARCHITECTURE FOR THE MTS NETWORK ADMINISTRATOR

9.1. UNIX Security Architecture

The UNIX Server features an integrated security architecture consisting of the following System Security Philosophy

The Security implementation is based on an approach to system security that emphasizes security configuration and control and detection of aberrant activities. The system security staff will use the features provided by the operating system and tool products to aid in the implementation and maintenance of the security configuration.

A system security configuration is based on the following tenets.

- Protecting and controlling root or equivalent “super-user” type privilege
- The */etc* directory is the administrative and security directory. No files with world write permissions will exist within this directory, and group write must only be permitted when required for normal operations
- Access control is maintained through aggressive configuration and audit trail monitoring
- Only the system approved file system objects and executable processes that are required to complete the operational mission are maintained on a System platform. No development tools must be maintained or available in the operational system environment
- The system unmask value will be maintained at 002 until such time that world-write is eliminated as a legacy application requirement. The root-user unmask will be maintained at 077 to avoid incidental occurrences of excessive permissions on root-created objects
- The *.rhosts* files must be populated only with net group names unless a legacy mission application requires additional information
- Auditing must be enabled for an approved list of audit flags developed for each system on all platforms and databases.
- Auditing must always occur for all users including the root-user
- Home directory permissions must be maintained at 775
- The root- or super-user must not be capable of direct login at the console or using network login mechanisms
- The finger and ftp network applications will be disabled. Recommend that network services be configured as recommended in the *UNIX Configuration Guidance for the DII COE Version 3.3*
- The network “snooping” commands must be disabled

FOR OFFICIAL USE ONLY

- Binary executables must be maintained at permissions of 111 (execute only). Shell executables, in particular set user ID (SUID) or set group ID (SGID) shell executables, must be maintained at permissions of 555 (read-execute)
- No login accounts must be maintained with a bogus default shell designation and locked password fields
- All encrypted password fields must contain either a locked password and/or encrypted password
- All password construction must include at least six unpronounceable alphabetic characters and two numbers or special characters
- Unknown or unapproved file systems must never be mounted in the operational System environment
- File system security and integrity is gained through sensible DAC and user privilege control (through user account and profile control mechanisms) management
- Primary misuse prevention is accomplished through the adherence to the security tenets
- Primary misuse detection is accomplished through the diligent examination of audit and security configuration compliance tool reports
- Database passwords must be unique and applied to the internal and external authentication mechanisms where required. No external password must be operationally maintained for the purpose of over-riding internal database authentication controls
- Establishing a standard countermeasure plan or operating procedure to execute when misuse is detected. Once abnormal behavior is detected, the countermeasure procedure is followed that identifies the who, what, when, where, and why of the access, corrects the anomalies, and then assesses damage

9.2. System Backup

System backups are also known as system saves. There are two types: full and incremental. A full backup makes copies of all designated files. The incremental backups copy those files that have been changed since the last incremental backup. The frequency of creating incremental backups is determined by the site.

Running a trusted facility requires full and incremental backups to ensure the system can be recovered to a known state and point in time. If a MTS Packet Switch becomes inoperable, it can be recovered by re-installing it from the backup MTS Packet Switch tapes.

Security managers must ensure that the backups are completed successfully and the results logged (i.e., normal or abnormal job termination). This double-checks that the backups were successfully completed. If the jobs did not end properly, they must be re-

run as soon as operationally possible. The backup medium (i.e., tapes) must be stored in a safe place so that if recovery is needed, the backup medium is available and useable.

9.3. System Restore

System restore is also known as system recovery. The tapes that were made during backups are used to restore the system. Restore operations may become necessary when files are deleted or damaged.

Before restoring data, the following steps must be taken:

- Ensure system and applications are intact
- Repopulate data using restore commands and the appropriate backup tapes
- Run security monitors and scripts and ensure the security configuration is intact

10.SYSTEM CONFIGURATION FILES

10.1. /etc./nswitch.conf

The *nswitch.conf* file orders the use of the various user/group authentication, host naming, and NIS databases by the system processes that use them.

The recommended ordering is:

passwd:	files nisplus
group:	files nisplus
hosts:	files dns nisplus #Requires resolv.conf setup for # DNS
name server lookup	
services:	files
networks:	files
rpc:	files
ethers:	files
netmasks:	files
bootparams:	files
publickey:	nisplus
netgroup:	nisplus
automount:	files nisplus
aliases:	files nisplus
sendmailvars:	files nisplus

10.2. IP Forwarding Control (/etc/rc2.d/S99INET)

The Solaris IP Forwarding capability provided in the */etc/rc2.d/S99INET* file must be altered so that IP Forwarding cannot occur. The setting for IP Forwarding must be set to “0” within the S99INET file. The following steps identify how to change this setting.

```
cd /etc/rc2.d
vi S99inet
/ndd -set
ndd -set /dev/ip ip_forwarding 1
{modify the 1 to be a 0}
ndd -set /dev/ip ip_forwarding 0
<esc>
<shift>:wq
```

10.3. Anti-Virus Software

10.3.1. McAfee Virus-Scan for Unix

McAfee Anti-Virus software for UNIX OS's is provided in segmented form. The ASSIST web site provides the McAfee Virus Scan product for UNIX OS's.

Shown here is the executable command line that is used to execute the McAfee software. The lines shown assume that the *uvscan* program is installed in /usr/local/bin.

/usr/local/bin/uvscan -m /etc/security configuration monitoring tool/anti-virus/infections --one-file-system -p -r --summary --verbose /

The options used are described here. The McAfee product supports other options that may be referenced in the *uvscan* manual page that is downloaded with the product software:

-m	Move infected files to directory
--one-file-system	Will not cross file system boundaries
-p	Preserve last access (a time) time
-r	Recursively scan directories
--summary	Summarize report results
--verbose	Verbose progress reporting

An example of the report contents follows:

Anti-Virus Scan Report

Sun Nov 2 15:21:39 GMT 1997

* Virus Scan for amhs

Files scanned	:	6183
Viruses detected	:	0
Viruses removed	:	0
Files removed	:	0
Files moved	:	0

=====

* Virus Scan for bigfoot

Files scanned	:	17413
Viruses detected	:	0

FOR OFFICIAL USE ONLY

Viruses removed : 0
Files removed : 0
Files moved : 0

* End Virus Scan Report

10.3.2. McAfee Virus-Scan for Windows NT

McAfee Anti-Virus software is used to protect the MTS Control Station and V2 from possible virus attacks. MTS utilizes version 4.5.0 of the anti-virus software. The configuration for the anti-virus software is shown below:

- Click on the **Start Menu**
- Select **Programs**
- Select **Network Associates**
- Click **Virus-Scan Console** to bring up the Virus-Scan Console window

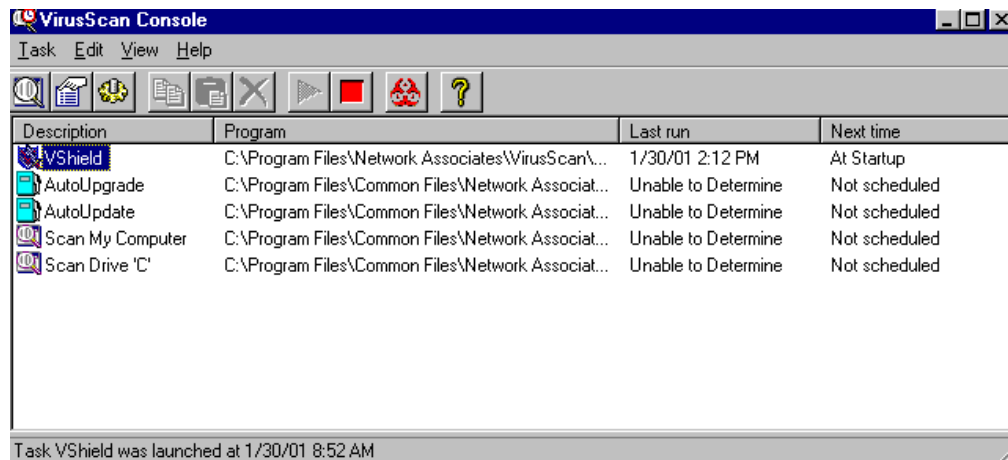


Figure 48 Virus-Scan Console

- Select **Vshield** from the list
- Click the **Run button** to enable Vshield when the workstation starts up
- Select **Vshield** from the list
- Click the **Configure button** to configure the settings for McAfee Anti-Virus
- Select the **Detection** tab

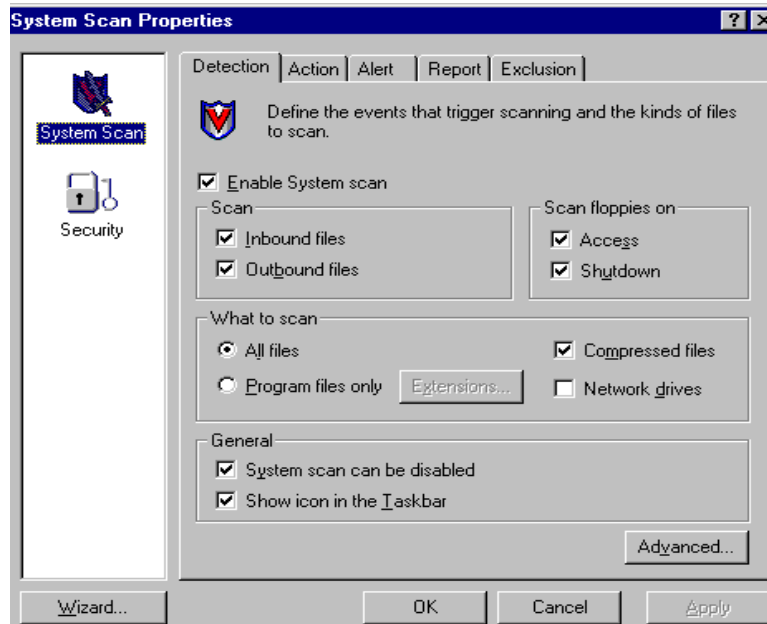


Figure 49 Virus-Scan Detection Settings

- Click the box marked **Enable System Scan**
- Click the box marked **Inbound files**
- Click the box marked **Outbound files**
- Click the box marked **Access**
- Click the box marked **Shutdown**
- Click the box marked **All Files**
- Click the box marked **Compressed files**
- Click the box marked **System scan can be disabled**
- Click the box marked **Shown icon in the Taskbar**
- Select the **Action** tab

FOR OFFICIAL USE ONLY

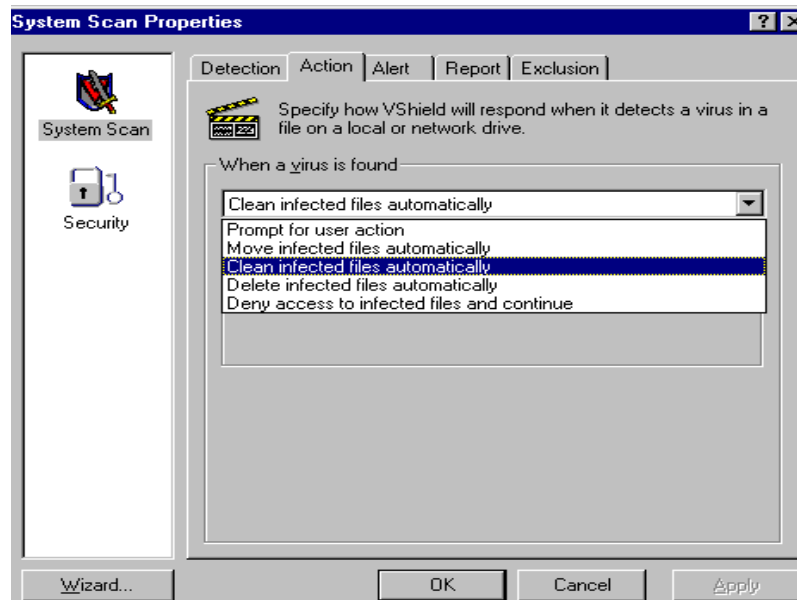


Figure 50 Virus-Scan Action Settings

- Click on the box **When a virus is found**
- Select **Clean infected files automatically** from the appearing list
- Select the **Alert** tab
- Click the box marked **Notify Alert Manager**

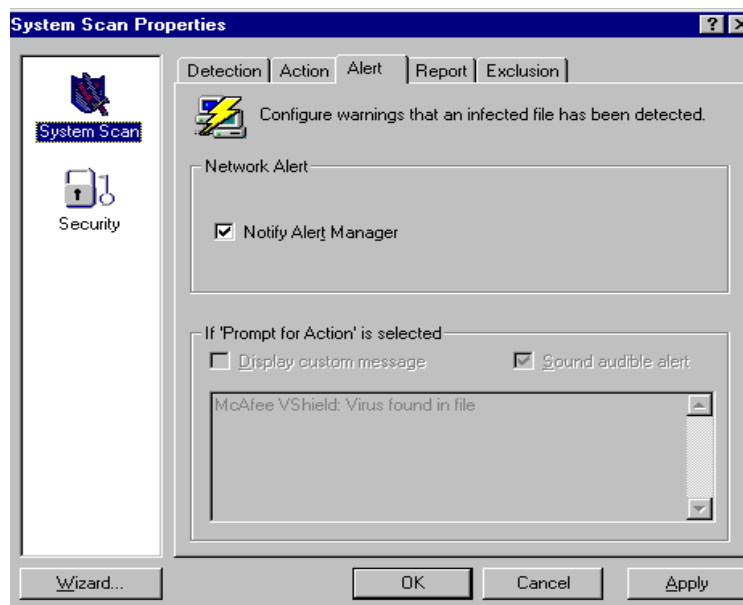


Figure 51 Virus-Scan Alert Settings

- Select the **Report** tab

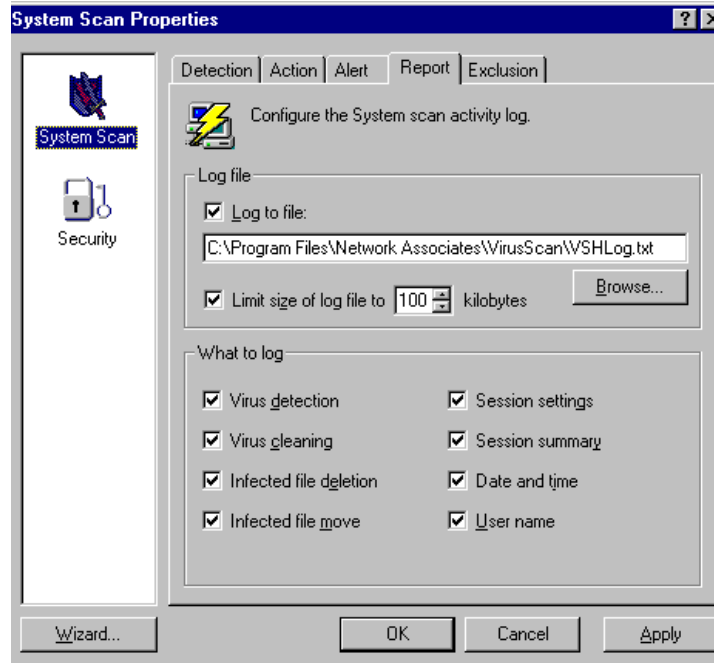


Figure 52 Virus-Scan Report Settings

- Click the box marked **Log to file** and ensure that the path for the log is *C:\Program Files\Network Associates\Virus-Scan\VSHLog.txt*
- Click the box marked **Limit size of log file to [100] kilobytes**
- Click the box marked **Virus detection**
- Click the box marked **Virus cleaning**
- Click the box marked **Infected file deletion**
- Click the box marked **Infected file move**
- Click the box marked **Session settings**
- Click the box marked **Session summary**
- Click the box marked **Date and time**
- Click the box marked **User name**
- Select the **Exclusion** tab

FOR OFFICIAL USE ONLY

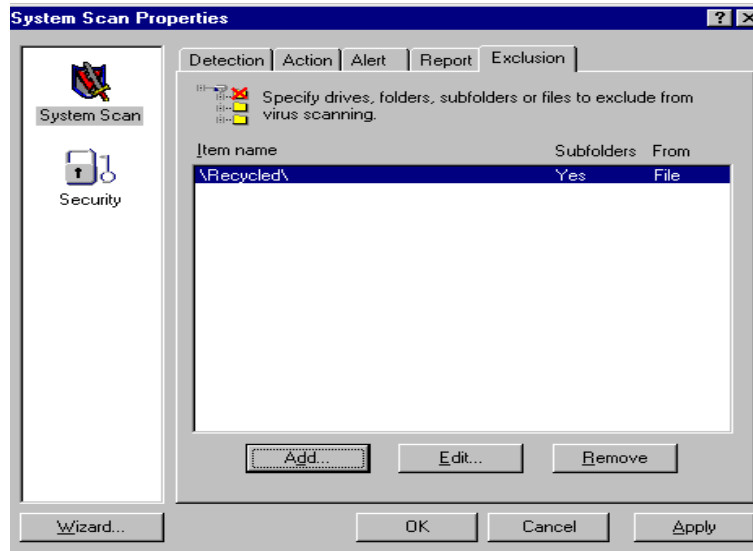
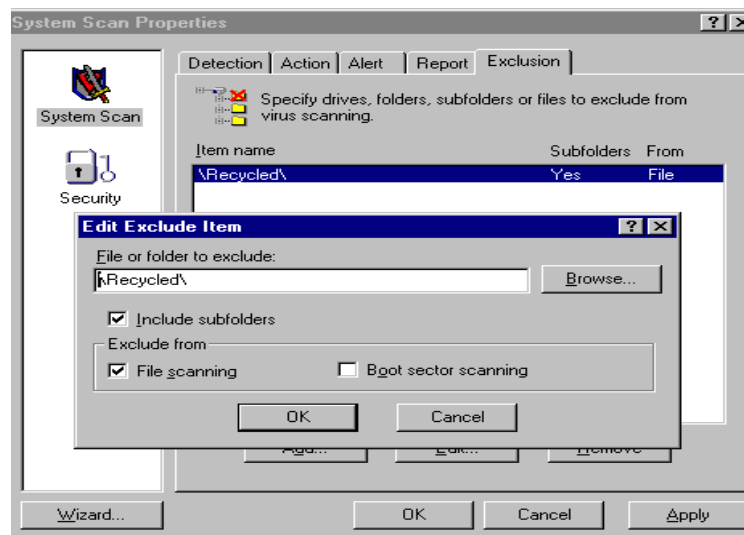


Figure 53 Virus-Scan Exclusion Settings

Ensure that **\Recycled** is the only item listed in the **Item name box**. Also ensure that it is marked as **Yes** for **Subfolders** and **File** for **From** in the same box.

If this is not listed then click the **Add button** and follow the steps below:

- Click the **Browse** button,
- Select the entry **Recycle Bin**
- Click the **OK** button.
- Click the boxes marked **Include subfolder** and **File scanning**.
- Click the **OK** button.



Editing Virus-Scan Exclusion Settings

- Click the **Apply button** and then the **Ok button**.
- Close the Virus-Scan Console window

10.4. Virus Definition Updates

New computer viruses are found almost daily. To ensure that MTS is not infected, virus definition files (dat files) must be updated a minimum of biweekly. This is in accordance with 380-19, Para 2-4c.

Approved updates can be found on the DISA homepage website. The URLs for the DISA homepage are as follows:

- Disa.mil (INTERNET)
- Iase.disa.mil (NIPRNET)
- Cassie.iiie.disa.smil.mil (SIPRNET)

Since MTS will not have Internet or network connectivity an administrator will have to download the anti-virus updates and place them on floppy disks for installation. The process for completing these updates to the Control Station and V2 are shown below in sections 10.4.1 and 10.4.2.

10.4.1. Control Station Installation

The control station is equipped with a floppy drive that will have to be installed prior to the installation of virus-scan updates.

- Download the file from one of the three websites noted above and according to your Internet connection.
- Copy the file to the A:\ drive or floppy drive
- Place the disk in the A:\ drive or floppy drive of the workstation being updated
- Click on **My Computer**
- Click on the **A:\ icon**
- Click on the update file (ex. 4117xdat.exe)



Figure 54 Installing Anti-Virus Updates

FOR OFFICIAL USE ONLY

- Click on the **next button** when the screen appears

NOTE: The file will be a self-executing file that will examine your system and will update all McAfee products to the latest definitions.

- Click on the **finish button** when the program is complete

10.4.2. V2 Installation

The V2 is a ruggedized laptop that has no hardware, network, or Internet connectivity. Due to these limitations, the virus-scan definitions do not need to be kept up-to-date since no virus could be introduced into its hard drive.

11. ACCESS CONTROL

The following sections describe these concepts as they relate to the MTS Packet Switch kernel.

11.1. Discretionary Access Controls (DAC)

File owners are responsible for controlling and protecting access to the files they own. The file owner may grant discretionary access on a need-to-know basis. Improperly controlled file access can permit unauthorized users access to information they do not have a need to know and can potentially compromise system security.

DAC must not be confused with classification or category designations that are assigned to system information and data. DAC allows an additional level of control over who may access information. It is designed to further limit access to information by allowing owners and groups of owners to establish access control over the information under their control.

11.2. Least Privilege Concept

The least privilege concept mandates that only the minimum amount of information or access to information that accomplishes a user's purpose be granted. For example, providing users of a system access to all information and world-read and -write permissions does not exercise the least privilege concept. Providing system users with read permissions, limited write permissions and no execute permissions for files within a group would be an example of exercising least privilege. Assigning access can be accomplished by manual executions of the administrative commands such as `chmod`, `chgrp`, and `chown`.

11.3. Assigning Permissions

Assigning permissions and/or privilege to file system objects must be done so that the least number of users have access to the information. It is recommended that write permission be restricted to the owner; or, if other users within the group require it, then write permission be granted to the group. Very seldom is it ever required to provide write permission to the world membership.

Each process and user is subject to a umask value that will automatically provide files that are created a set of permissions that are by default 775.

11.4. Set UID and Set GID Programs

Certain programs require special privilege during their operation. Within the UNIX operating environment, it is possible to cause a program to change its effective ID to operate with the privileges of another user or group. This is the purpose of the SUID and SGID mechanisms. SUID and SGID functions add value to the system in that they allow privileged functions to be performed without disclosing real root ID or group membership. However, without the proper precautions, SUID and SGID programs can provide ways to subvert the special privileges for unauthorized uses.

FOR OFFICIAL USE ONLY

The security staff must maintain knowledge of the SUID and SGID programs that exist on the system. It is important to recognize any modifications to existing programs or newly added SUID/SGID programs on the system. The only permission assignments acceptable for SUID and SGID programs must be read-execute (555) for owner, group, and world.

12. SECURITY-RELEVANT FILES AND DIRECTORIES

Several directory hierarchies are considered critical to the system and security administration. These hierarchies must be monitored and maintained to ensure that the general user community can neither accidentally or maliciously cause damage to the system operation by manipulating the key configuration files within them.

12.1. /(root) Directory

The root directory is the home directory for the root-user and the parent for all hierarchies in the file system. The root directory is often the target of attacks and Trojan programs.

The root-users home directory contains several files that make up the root-users operating environment, such as *.profile*, *.xsession*, etc., that can provide opportunities for a malicious user to subvert root privilege. The root directory does not require a *.rhosts* file and the MTS Packet Switch security configuration requires no *.rhosts* exist in this directory. The environment startup files, *.profile*, *.login*, *.xsession*, *.cshrc* will be assigned permissions of read-write-execute for the owner and no permissions for group or world (700).

The security staff must be aware of and investigate modifications or additions to this directory.

12.2. /etc Directory

The */etc* directory is the primary administrative and security directory on the UNIX file system. The files and directories in this directory directly affect the startup, configuration, and operation of the system and must be monitored, maintained, and protected accordingly. The rule of thumb for the */etc* directory is that no world-write permissions are assigned to any of its files or directories.

12.3. Binary Files

There are binary files on the system that require special attention either because of the information produced or because of the additional privilege gained during execution. Below are files that must be monitored.

Table 7 Binary Files

File	Owner	Group	Permissions
/bin/ps	root	sys	4755
/bin/pstat	bin	sys	2755
/usr/bin/lav	bin	sys	2755
/usr/bin/X11/xterm	bin	bin	755

FOR OFFICIAL USE ONLY

File	Owner	Group	Permissions
/usr/sbin/snoop	root	bin	500
/usr/sbin/admintool	bin	bin	500

12.4. Audit Logs and Online Archives

The permissions on all audit control files must be set to only allow write access to root. All audit programs and processes require root privilege to operate.

12.5. Other Relevant Files

Below is a list of other security-relevant files and the permissions for the files.

Table 8 Other Files

Pathname	Owner	Group	Permissions
/usr/etc/ncstats	bin	sys	2755
/usr/bin/nfsstat	bin	sys	2755
/usr/etc/rpcinfo	bin	bin	755
/Unix	root	sys	644
/tmp	root	sys	1777
/var/nis	root	sys	755
/var/nis/*	root	sys	644

12.6. Unauthorized File System Objects

The MTS Packet Switch and mission system must be maintained as a controlled software environment. This means that the only software that may be used on the system platforms will go through a configuration management control processes, or be authorized for use through the appropriate security authority for the system in question. Software that is not part of this baseline must not be permitted on the operational system without approval. The following software is authorized for the V2 and Control Station and is considered mission critical:

- Windows NT 4.0, SP6a, accessories, and hot fixes
- MTS Messenger 2.06
- Windows NT 4.0, SP6a

- MTS Messenger 2.06
- Tracerlink Pro 2.0.11
- McAfee Virus Scan 4.0.5
- Tracerlink Pro 2.0.11
- McAfee Virus Scan 4.0.5
- Adobe Acrobat 5.0
- Inside Out Networks Drivers 1.26

12.7. Development Tools and Utilities

Operational systems must not be permitted to maintain development tools such as compilers, linkers, debuggers, etc., on the file system or on the inter-network system. Tools that are required must be restricted to and maintained on systems that do not connect with the networked operational system components.

12.8. Non-MTS Packet Switch Specific Software

The MTS Packet Switch operational systems must not have software unless authorized through the proper authority loaded or installed.

12.9. .rhosts Files

The *.rhosts* file allows a host to host connection ability based either on host IP or account identity or both. The *.rhosts* file contains this information and must be carefully monitored and maintained by the security staff. Many application programs utilize NFS and RPC commands to automate required connectivity and to make the connectivity transparent to the user community. Three things must be considered when using the *.rhosts* mechanism:

- It must be controlled
- It must be monitored
- It must never be used in the root directory

The most assured way to use the *.rhosts* mechanism is in conjunction with the NIS+ high security mode and NIS+ netgroups capability. With NIS+ in place, and very few exceptions, every *.rhosts* file must contain an entry reflecting the netgroup name chosen for the site's mission suite..

The *.rhosts* file in all other home directories must not be permitted to allow world access; a permissions set of 750 is strongly recommended, 600 provides more assurance. An *.rhosts* file is located in each users directory that requires this file. Using the MTS Packet Switch account creation features, this file is copied into the home directory during account creation as covered in the next section.

FOR OFFICIAL USE ONLY

An alternative method for the location of the *.rhosts* file is in the */etc* directory, owned by root, group of root, and a permission set of 440. This *.rhosts* file becomes the central *.rhosts* file from which the security staff can maintain strict connectivity rules. This *.rhosts* file may be linked to from each users' home directory. In this manner, the usefulness of the *.rhosts* file can be obtained while limiting its inherent security risks. Combined with the NIS+ netgroups, this is a stronger security mechanism for controlling NFS and RPC capabilities. This method is effective, but also requires maintenance to ensure that all required connectivity is granted while no unauthorized connections are allowed.

The careful monitoring of *.rhosts* file permissions and content must be required to ensure that unauthorized connections are not enabled.

The *.rhosts* file must not be permitted to be used in the root (*/*) home directory. However, it is strongly recommended that a null (empty) *.rhosts* file be maintained in the root directory, owned by root, group of root, and a permission set of 400. This will remove the possibility of a non-root process writing to the file.

13. MOUNTED FILE SYSTEM CONTROL

Sharing and mounting file systems to the MTS Packet Switch must be limited to file systems that are specifically identified and required for the normal operation of the system. Unknown or undefined file systems are never to be mounted on the operational networks.

Mount operations provide the mechanisms required to control access to a shared file system. Refer to the operating system documentation for the mount command options. The mounted file systems are controlled in much the same way as files and directories on the file system using user and group IDs, and permissions to control read and write. In fact, the file system is an extension of one system's information to another. The only differences are the format of the "sharing" command and the fact that the permissions assigned at this level are used to control the entire file system. The assignment of the file system permissions to restrict certain types of access to the system in most cases overrides the file and directory permissions on the file system itself.

Of particular concern is sharing file systems having unlimited permissions with those who might mount the file system. This sets up a "trust" relationship between the system sharing the file system and all who choose to mount the file system, allowing anyone to modify its content.

The NIS+ credentials provide a secure method of establishing a connection via the NFS function. This method also requires that the host and user names be populated into a NIS+ Netgroup. The NIS+ Netgroup name must be required to be used in all exported directory command lines contained in the */etc/dfs/dfstab*. This extends the secure RPC trust to all included hosts and users and denies access to any host or user not included.

13.1. User Privileges

Privileges are granted that enable the user to access the tools required to perform the task. The granting of privileges is controlled using the "least privilege" concept. This philosophy provides that users are must be given only the amount of privilege required to complete assigned tasks. Within UNIX based systems this is accomplished by controlling Group Accounts and Profiles.

In UNIX systems, the privileges are broken into two categories, root- and normal-user. Root privilege allows unlimited access to all file system resources, normal system, and root privilege commands. The normal user is granted access to system resources and normal commands by virtue of assigned user and file system permissions. While permissions allow for a great deal of (discretionary) control over the file system resources, they provide no control over the system command features. A user will not have root privilege. The SA and security managers both require the root privilege in order to perform the role-related tasks.

To make security management easier, two distinct positions have been identified:

- The Site Designated Approval Authority (DAA) who has overall responsibility for the trusted facility's security

FOR OFFICIAL USE ONLY

- The site information assurance security officer (IASO), who has detailed technical knowledge of the workings of the System components' security mechanisms, and configuration and maintenance of the secure network

These persons acting together manage the security of the System. The Site DAA and the Site IASO may delegate some or all responsibilities to other qualified individuals, as appropriate.

Having taken these steps, the security staff must have the data and information necessary to determine the account identification and damage done to the system. It is important to document these findings. The security staff may also be required to manually search for additional areas of penetration Site Composition

It is important to understand the nature and topology of the site system configuration. Every physical and logical access point into the trusted MTS Packet Switch facility becomes the responsibility of the information security staff regardless of the physical location of the accessing host computer.

14. LOCAL ACCOUNTS

Local accounts limit user access to the machine onto which they are logged onto MTS. They do not have access to network information services (NIS).

15. SITE-SPECIFIC RESPONSIBILITIES AND PROCEDURES

15.1. Site Chief/Commanders

The site commander will be responsible for establishing a security plan in their command and ensure that the following are accomplished:

- Establish and manage the ISS command program to include defining the ISS personnel structure and directing the appointment.
- Promulgate ISS guidance within each command, to include developing command unique guidance as required
- Ensure that personnel are properly trained

15.2. Direct Approving Authority (DAA)

The DAA for the MTS is the Program Executive Office (PEO), Standard Army Management Information Systems (STAMIS). As such, he or she formally accepts the level of residual risk for the operation of the MTS and officially declares that adequate safeguards are in place against security threats. Any issues concerning the MTS security are decided by the DAA.

15.3. Information Assurance Security Officer (IASO)

For each MTS or group of MTS, there will be an IASO appointed by the commander or manager of the activity responsible for the MTS. The same IASO may be appointed for multiple MTSs, particularly in the environment where they are oriented toward the functional user as the operator. The following paragraphs briefly describe the MTS IASO, responsibilities of the position, and his/her relationship with the MTS user.

There are several positions that have significant roles in network and computer security but in this respect, the IASO is generally most important to the user. The IASO is the day-to-day network and computer security person for the MTS. He or she (or their designated representative) is the first person users must try to contact if they have a computer-related security problem or issue.

The IASO responsibilities may vary slightly from location to location, but the following are typical, especially for the MTS IASO. The IASO:

- Ensures systems are operated and maintained according to the established procedures and regulations
- Is the focal point for all assigned system security matters
- Provides end-users with system-specific and general awareness security training
- Ensures managers, system administrators, and users have the appropriate security clearances, authorization, and need-to-know
- Conducts security threat and vulnerability assessments of the MTS PCs

FOR OFFICIAL USE ONLY

- Monitors system activity, including the identification of the levels and types of data handled by the MTS, the verification of password assignments, and the review of audit trails, outputs, etc., to ensure compliance with the MTS security policies and procedures
- Reports security incidents and technical vulnerabilities to the DAA, the MTS General Manager and the MTS Program Manager
- Maintains access control records and establishes an access control policy in which only authorized personnel can gain access to the system
- Establishes a system for issuing, protecting, and changing system passwords
- Prepares or oversees the preparation of certification and accreditation documentation
- Maintain accreditation documentation and initiate re-certification and re-accreditation when changes affecting security have occurred
- Implementing appropriate safeguards required by directive
- Completing an AIS security survey for the MTS and developing the MTS SSOP
- Supports user training, in accordance with the MTS security policies and procedures, and in accordance with the system security requirements specification (SSRS)
- Assists in the development, implementation, and testing of the MTS contingency and incident response plans
- Ensures that only authorized personnel can gain access to the system
- Maintains close liaison with system administrators to promote security at all levels of system operations

15.4. System Administrator (SA)

The system Administrator (SA) is required to keep the MTS operational and the system secure. The following tasks are essential in accomplishing these goals:

- Ensure that the operating system for the MTS is configured properly and that the security features appropriate to the intended level of system operation are properly set. Such settings must be periodically reviewed; such reviews will not involve looking at information or data contained in the files of individual users other than system configuration files
- Periodically check with the operating system manufacturer, the LIWA, in order to keep informed of system security problems and patches as they are developed, and apply them as appropriate in order to maintain security
- Review file names, length, permissions, and directories. If any of this information leads a SA to suspect that an individual user is misusing the system or engaging in other misconduct, the SA will notify the chain of command

FOR OFFICIAL USE ONLY

- If a SA suspects an unauthorized user is attempting to access the MTS, the SA is authorized to take the actions necessary to verify and limit the penetration attempt from an unauthorized user. Once verified, the SA will notify, concurrently, the chain of command. The SA may conduct a system backup of appropriate log, history files, and user directories. Once the SA has determined that the anomaly is in fact an unauthorized intrusion, the SA will not in any other manner specifically target, track or attempt to investigate a suspected intruder's activities except as part of a properly authorized investigation.

15.5. Network Administrator (NA)

The network administrator (NA) operates under similar broad authority and restrictions as the SA. While it is the NA's responsibility to keep the networking infrastructure operational and secure, they operate under the same constitutional and statutory controls as the SA. These restrictions represent a balance between the actions necessary to provide a reliable and secure communications backbone for the MTS, while at the same time ensuring the privacy rights of the users. It is the goal of the NA to ensure the continued operation infrastructure is composed of two major components-the communications medium (which is under their control) over which the MTS communications travel; and the network hardware (that is, hubs, switches, etc.,) which make up the physical equipment of the network. The following tasks are critical in achieving the goals of continuity and security:

- Ensure that all hardware and software components of the network infrastructure are properly configured and the security features and controls appropriate to the intended level of system operation are properly set. Such settings must be periodically reviewed to ensure that they are set correctly and have not been modified without the network administrator's knowledge
- Periodically check with the maker of the network components, the LIWA, and/or the DISC4, in order to keep informed of system security problems and patches as they are developed, and apply them as appropriate to maintain the integrity of the network
- Use network management systems to monitor the operational status of the network, and to collect statistics on bandwidth utilization and error rates
- If the NA suspects that an individual user is engaging in any misuse or misconduct, the NA will notify, concurrently, the appropriate Government representative. The NA will not specifically target or track an individual's activities except as part of a properly authorized investigation
- If the NA suspects an unauthorized user is attempting to access a system on the network, the NA will notify, appropriate Government representative. The NA will not specifically target, track, or attempt to investigate a suspected intruder's activities except as part of a properly authorized investigation
- Use sniffers or network analyzers only as tools in diagnosing network problems

15.6. Users

Owners, developers, operators and users of the MTS each have a personal responsibility to protect the system's resources. Functional managers have the responsibility to provide appropriate security controls for any information resources entrusted to them. These managers are personally responsible for understanding the sensitivity and criticality of their data and the extent of losses that could occur if their sources are not protected. Managers must ensure that all users of their data and systems are made aware of the practices and procedures used to protect the information resources.

General Responsibilities - All MTS users share certain general responsibilities for information resource protection. The following considerations must guide user actions:

- Treat information as you would any valuable asset. You would not walk away from your desk leaving cash or other valuables unattended. Take the same care to protect information. If you are not sure of the value or sensitivity of the various kinds of information you handle, ask your IASO for guidance
- Observe established policies and procedures. Specific requirements for the protection of information have been established. These requirements may be found in policy manuals, rules, or procedures. Ask your IASO if you are unsure about your own responsibilities for protection of information
- Recognize that you are accountable for your activities on the MTS. After you receive authorization to use the MTS, you become personally responsible and accountable for your activity on the system. Accordingly, your use must be restricted to those functions needed to carry out job responsibilities
- Report any unusual occurrences. Many losses would be avoided if users would report any circumstances that seem unusual or irregular. Warning signals could include such things as unexplainable system activity that you did not perform, data that appears to be of questionable accuracy, and unexpected or incorrect processing results. If you must notice anything of a questionable nature, bring it to your IASO/SA attention

Security and Control Guidelines - Some common-sense protective measures can reduce the risk of loss, damage, or disclosure of information. Following are the most important areas of information systems controls that assure that the system is properly used, resistant to disruptions, and reliable:

- Make certain no one can impersonate you. A password is used to verify the user's identity, this is the key to system security. Do not disclose your password to anyone, or allow anyone to observe your password as you enter it during the log-on process. If you choose your own password, avoid selecting a password with any personal associations, or one that is very simple or short (See Password Generation for rules on how to create a password). The aim is to select a password that would be difficult to guess or derive. "1REDDOG" would be a better password than "DUKE"
- If your system allows you to change your own password, do so regularly. Passwords on the MTS are required to be changed at least semi-annually. Periodic

FOR OFFICIAL USE ONLY

password changes keep undetected intruders from continuously using the password of a legitimate user.

- After you have logged on, the computer will attribute all activity to your user id. Therefore, never leave your terminal without logging off -- even for a few minutes. Always log off or otherwise inactivate your terminal so no one can perform any activity under your user id when you are away from the area
- Safeguard sensitive information from disclosure to others. Often and individual forget to lock up sensitive reports and computer media containing sensitive data when they leave their work areas. Information carelessly left on top of desks and in unlocked storage can be casually observed, or deliberately stolen
- While working, be aware of the visibility of data on your personal computer or terminal display screen. You may need to eliminate over-the-muster viewing
- Label all sensitive diskettes and other computer media to alert other employees of the need to be especially careful. When no longer needed, sensitive information must be deleted or discarded in such a way that unauthorized individuals cannot recover the data. Printed reports must be finely shredded, while data on magnetic media must be overwritten. Files that are merely deleted are not really erased and can still be recovered
- When data is stored on a hard disk, take steps to keep unauthorized individuals from accessing that data
- Maintain the authorized hardware/software configuration. Computer "viruses" acquired through seemingly useful or innocent software obtained from public access bulletin boards or other sources has affected some organizations; others have been liable for software illegally copied by employees. The installation of unauthorized hardware can cause damage, invalidate warranties, or have other negative consequences. Install only hardware or software that has been acquired through normal acquisition procedures and comply with all software licensing agreement requirements
- Observe the copyright laws for all computer data

16. COUNTERMEASURE PROCEDURES

Each site must develop countermeasures procedures to address what to do when misuse is suspected and/or detected. There are no hard and fast rules in resolving an act of misuse caught in the act; however, here are the general guidelines:

- Identify the account, under which the misuse has been perpetrated
- Identify the damage done and/or information compromised
- Document the occurrence and save the evidence defining the misuse

The information provided here must be applied in accordance with the site policy and procedure

16.1. Controlling Misuse

Misuse of the DoD systems is illegal and protected under federal and local statutes. The site security staff is responsible for maintaining the security posture of their system. This requires the security staff to understand security procedures during routine, exception, and contingency periods of operation. The first steps toward controlling misuse are education, training, and exercises.

16.2. Software Controls

The MTS Packet Switch must be continually monitored to verify that the security configuration is maintained.

16.3. Misuse Detection

You can use the Event Viewer to check for odd logon entries, failures of services, or odd system restarts.

Check for odd user accounts and groups. You can use the User Manager tool. Ensure that the built-in GUEST account is disabled if the system does not require guest access.

Check all groups for invalid user membership. Some of the default NT groups give special privileges to the members of those groups. Members of the Administrators group can do anything to the local system. Backup operators can read any file on the system. PowerUsers can create shares.

Look for invalid user rights. To examine user rights use the User Manager tool under Policies, User Rights. There are 27 different rights that can be assigned to users or groups. Generally the default configuration for these rights is secure.

Check to see if unauthorized applications are starting. There are a number of different methods an intruder could use to start a back door program, so be sure to:

- Check the Startup folders. Check all items in c:\winnt\profiles*\start menu\programs\startup folders. You can also examine all the shortcuts by selecting Start, Programs, Startup. Note that there are two startup folders, one for the local user and one for all users. When a user logs on, all of the applications in

FOR OFFICIAL USE ONLY

both the "All Users" and in the users startup folder are started. Because of this it is important to check all of the startup folders for suspicious applications.

- Check for invalid services. Some backdoor programs will install themselves as a service that is started when the system boots up. Services can then run as any user with the "Logon as Service" user right. Check services that are started automatically and be sure that they are necessary. Also check that the services executable file is not a Trojan horse or backdoor program.

Check your system binaries for alterations. Compare the versions on your systems with copies you know that have not been altered, such as those from your initial installation media. Be cautious of trusting backups; they could also contain Trojan horses.

Using anti-virus software will also help you check for computer viruses, backdoors, and Trojan horse programs. But remember that malicious programs are continuously created, so it is important to keep your anti-virus software up to date constantly.

Check for any jobs scheduled to run. Intruders can leave back doors in files that are scheduled to run at a future time. This technique can let an intruder back on the system (even after you believe you had addressed the original compromise). Also, verify that all files/programs referenced (directly or indirectly) by the scheduler and the job files themselves, are not world-writable. To check for jobs currently pending use the "at" command or the WINAT tool from the NT resource kit.

Look throughout the system for unusual or hidden files. These can be used to hide tools and information (password cracking programs, password files from other systems, etc.). Hidden files can be seen with the NT Explorer. Select View, Options, Show all Files. To view hidden files at the command prompt type `dir /ah.`

Check for altered permissions on files or registry keys. Part of properly securing an NT system is to set the proper permissions on files and registry keys so that unauthorized users cannot start unauthorized programs (eg. backdoors or keyloggers) or change system files.

Check for changes in user or computer policies. Policies are used on NT systems to define a wide variety of configurations and can be used to control what users can and cannot do. Since a number of items are configured in the policy editor (poledit.exe) it is recommended to keep a current copy of the policies you create in case they are altered and you need to determine what was changed.

17. ROOT ACCOUNT USAGE

No one must use the built in root or administrator accounts to accomplish the day-to-day mission work on the system. Each user with administrative duties must have a uniquely identifiable account so that any administrative work can be tracked back to that individual. Shared accounts are not allowed under any circumstances.

The root account must be reserved for the maintenance of the system and for certain system security-relevant functions. The root privilege must be tightly controlled and given to only those administrative personnel who specifically require the privilege to accomplish their duties and responsibilities, i.e., the privilege must be invoked to carry them out. Standard procedure must be to log on as a normal user and then *su* to root.

18. AUDIT MANAGEMENT

18.1. Audit Strategy

The actual MTS Packet Switch hardware platforms and OSs being used are site dependent and consist of at least one server, having the capability to generate audit data. Site security and administrative personnel must plan the platform provides sufficient space to support daily audit trail collection.

The system shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the system so that read access to it is limited to those who are authorized for audit data. The system shall be able to record the following types of events: use of identification and authentication mechanisms, introduction of objects into a user's address space (e.g., file open, program initiation), deletion of objects, and actions taken by computer operators and system administrators and/or system security officers, and other security relevant events. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/authentication events the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name of the object. The ADP system administrator shall be able to selectively audit the actions of any one or more users based on individual identity.

18.2. Audit Definitions

Before discussing the audit management concepts further, some terminology definitions are in order:

- **Audit Event:** This is a name that is normally synonymous with a security-relevant activity, such as a file open event, or an su usage, etc.
- **Audit Class:** This is a grouping of audit events that have a common theme, such as the administrative class that groups the administrative events such as suchmod, etc.
- **Audit Record:** This is a collection of information for an audit event. The audit record contains data and time, user, object, and event information.
- **Primary Audit Trail File:** This is normally selected as the first audit trail file where audit records are stored (the location is also referred to as the audit depository. If selected, this is the active audit trail.
- **Secondary Audit Trail File:** This is normally selected or "switched to" as the second audit trail file where audit records are stored when the primary audit trail file reaches capacity. If selected, this is the active audit trail and may also be referred to as the audit depository.
- **Audit Online Archive:** The audit online archive is a centralized location where all past day, inactive daily audit trail files are stored.

FOR OFFICIAL USE ONLY

- **Audit Long Term Archive:** The audit long-term archive is the permanent storage media that will be used to store the audit trails.

18.3. Audit Online Archive

The audit trails on each platform must be moved out of the daily audit depository directories on a daily basis. This activity ensures that the audit trail depository has the space required to support each day's audit trail requirement. It is recommended that an online archive be maintained where the daily audit trails may be moved. The online archive is designed to provide the workspace required to perform the audit trail analysis. The length of time that the files are maintained within the online archive must be the minimum time required to analyze the audit trail files. The recommended minimum time is 10 days if space permits. Once an audit trail file is analyzed, it is moved to the long-term archive.

18.4. Audit Long Term Archive

The audit long-term archive is required to provide long term storage for the audit trail files collected. The long-term archive storage media must be suitable to maintain the data for the period of time required for audit trail archiving. The system's *Security Procedures Manual* must provide the length of required archive storage. The minimum long-term archive storage time period considered must be two years.

18.5. Archive Labels

Each long-term storage media container must be marked with the following information:

- System Name
- OS Version
- Start Date
- Stop Date
- Classification
- Date Archived

The long-term archive media must be stored in accordance to the procedures defined in the DODI 5200.1-R.

18.6. Audit Depository Space Full Conditions and Policy

The auditing system on all platforms is required to be configured in such a way that filling the audit depository space to capacity does not disable the system. The configurations recommended for the MTS Packet Switch platforms attempt to curtail this kind of problem but are not a guarantee that a scenario cannot occur that might cripple the system. For example, it must be noted that, in some cases, filling the audit depositories might indirectly cause the system to be disabled or at least severely impaired. This is dependent on where the audit depository is located on a system. For example, if the audit depository is located on a root file system hierarchy (that is already

FOR OFFICIAL USE ONLY

overburdened) and reaches a point of saturation, the system could enter a “hung” state because of resource starvation.

The only assured method of ensuring that the system remains in a good operational state is to monitor the system console messages. In the case of the auditing mechanism, ensuring that the audit configuration is correct and especially that, any audit warnings received concerning the state of the audit trail depository space are heeded and appropriate actions are taken.

It is recommended that the auditing monitor programs on the platform auditing systems employed by MTS Packet Switch must be configured to notify the security staff when the audit depository space depleted reaches 85% of the partition capacity.

18.7. Audit Event Requirements

Auditing a carefully chosen but minimal set of required events will provide the security staff with the information required to track the most important security-related activities but limit the cost to the system and security staff resources. The minimal set of security-related activities that must be audited in MTS Packet Switch systems are shown below.

Table 9 Audit Requirements

Activity	Security-Related Event
Login and logout activities	Local login/logout
	FTP
	rlogin
	rsh
	rexec
	rex
	passwd
Administrative activities subset	change mode/permissions
	change ownership
	reboot
	hostname setting
	time of day setting
	real unique identifier modification
	real group identifier modification
	system shutdown

FOR OFFICIAL USE ONLY

Activity	Security-Related Event
	creating a directory/folder
	removing a directory/folder
	mounting a file system
	unmounting a file system
	network domain name setting
Failed object deletion activities	unlinking an object
	renaming an object
	truncating an object
	open with any combination of truncate, create or write modifiers
Failed object write activities	open with any combination of truncate, create or write modifiers
Failed object creation activities	open with any combination of truncate, create or write modifiers
	object creation
	linking an object
	changing directories
	symbolic linking
	rename an object
	create a directory
	remove a directory
Failed object read activities	reading a link
	all open calls

The previous table contains the minimum recommended set of security-related events that are required to be monitored. Site policy may add to this set, but must not subtract from it.

It is strongly recommended that the minimum set of required audit events must be enabled for all users of the system, including root.

18.8. Audit Log Analysis

MTS audit logs must be reviewed on a weekly basis. There may be situations such as suspected or actual system misuse (i.e., hackers), which require an even more frequent audit log review. In reviewing the audit logs, the security staff must look for unusual

FOR OFFICIAL USE ONLY

activity such as repeated failed attempts to access the system. Some other activities that the security staff must look for are attempts to use privileged commands, change file permission, access sensitive files, and system accesses by personnel at non-standard working hours.

19.CHANGE DES KEYS

To change DES keys with the `chkey` command, you need modify rights to the domain's Cred table, the password from which the entry in the Cred table was formed, an entry in the domain's Passwd table, and the login password. The sequence is as follows:

- rootmaster% **keylogin**
- Password: <enter-current-password>
- rootmaster% **chkey**
- Updating nisplus publickey database
- Generating new key for 'unix.53456@Wiz.Com'.
- Enter login password: <enter-new-password>
- Retype password: <re-enter-new-password>
- Done.

The `keylogin` command helps authenticate an NIS+ principal. When a principal logs in, the login process prompts for a password, which is used to authenticate the principal. Normally, this is the only time the principal is asked to provide a password. However, if the principal's DES credentials were created with a password that is different from the login password, the login password will no longer be able to authenticate the principal.

To remedy this problem, the principal must perform a `keylogin`, using the `keylogin` command, after every login. The `keylogin` command prompts the principal for its network password and stores it in the key server. From there, it is used by all NIS+ processes to authenticate the principal.